tenable RESEARCH

TENABLE'S 2021 THREAT LANDSCAPE RETROSPECTIVE

A guide for security professionals to navigate the modern attack surface

Table of Contents

FOREWORD **3**

EXECUTIVE SUMMARY **4**

KEY TAKEAWAYS **5**

METHODOLOGY **6**

INTRODUCTION **7**

SECTION 1: VULNERABILITY LANDSCAPE **8**

Microsoft Exchange Vulnerabilities 8

Print Spooler 9

Zero-Day Vulnerabilities 11

Still VPNs 13

Other Vulnerabilities of Interest in 2021 15

SECTION 2: THREAT LANDSCAPE **20**

Supply Chain 20

Ransomware 22

Breaches 24

CONCLUSION **28**

SECTION 3: A CLOSER LOOK AT THE KEY VULNERABILITIES IN 2021 ..... **29**

Foreword

Let's break some patterns

Turbulent. Can you think of a better word to describe 2021? I can't.

As we were putting the finishing touches on the 2021 Threat Landscape Retrospective, the cybersecurity industry was rocked by the revelation of a critical vulnerability in Apache Log4j 2, a widely used Java logging library. The vulnerability, dubbed Log4Shell, emerged as cybersecurity professionals continued to grapple with fallout from the COVID-19 pandemic.

Now in its second full year, the pandemic has triggered unprecedented changes in how we all live and work. We saw organizations around the world embracing remote work models, transforming how we define "the perimeter." We watched as the pace of digital transformation accelerated, driving the mass migration of mission-critical applications to the cloud. And we observed as attackers continued to make effective use of the age-old tactic of daisy chaining vulnerabilities to facilitate ransomware attacks and breaches like SolarWinds and Kaseya, all of which served to remind us how risky the software supply chain has truly become.

Yet, even in the midst of all this turbulence, we are frustrated by all the many things that haven't changed enough in 2021. We've seen far too many organizations still trying to apply traditional cybersecurity tactics to modern deployments of cloud infrastructure. We've seen far too many legacy vulnerabilities still being left unpatched, even when they're known to have been actively utilized by attackers to gain entry to an organization's environment. And — as Log4Shell makes clear — we've seen organizations overlooking obvious points of security failure throughout their software supply chain, from the initial creation of code to how updates are deployed to users.

This retrospective is intended to help security professionals make sense of the morass of threats and vulnerabilities that made 2021 an especially risky year. It's intended as a clear reminder that practicing cybersecurity fundamentals — including finding and fixing critical vulnerabilities and addressing misconfigurations in the cloud and Active Directory — is more important than ever. We want to bring to light the sheer scope of the challenge security organizations face, in hopes that it will spark discussion that will lead to true, lasting change in how cybersecurity is managed.

We believe a new approach to cybersecurity is warranted. The way forward requires not only remediating vulnerabilities in the products your organization deploys but also finding the means to continuously evaluate the trust relationships within your environment to develop a clearer understanding of how they might be exploited. Now that cloud adoption has rapidly increased and organizations are embracing the flexibility that cloud-native infrastructure provides, it is vital to find and fix every flaw before deployment. The reliance on code libraries has led to software flaws being replicated ad infinitum. By the time software reaches run-time, it's already too late. It's long past time for detection to move from reactive to proactive, so that security teams don't have to wait for infrastructure to be created in order for them to discover and mitigate vulnerabilities in code. It's time for GitOps to be seen as the de facto universal for a wide variety of operations to manage entire workflows. Merging GitOps and Infrastructure as Code approaches will allow organizations to take a security-first approach to codifying how their servers should operate, as well as offering security teams visibility into the entire line of operations.

With the traditional perimeter atomized by remote work, it's essential for all organizations to begin addressing cybersecurity at the source by "shifting left" and embracing a culture of DevSecOps. It's time to embrace new approaches to cybersecurity that break the patterns of the past and empower security professionals to play a role in reducing risk at all stages of software development.

Renaud Deraison

Co-founder and Chief Technology Officer

Tenable

Executive Summary

The past year certainly had more than its fair share of headline-grabbing attacks and vulnerabilities. Tenable's Security Response Team (SRT) saw several cyberattacks cross the chasm from the digital world to the physical, rattling the public's faith in fuel and food supply chains, among other unpleasant outcomes. And, as we were finalizing this year's Threat Landscape Retrospective in December 2021, security practitioners were having their holiday season disrupted by the Log4Shell vulnerability in Apache Log4j 2, a widely used Java logging library. As Tenable's CTO Renaud Deraison states, this vulnerability reveals troubling fissures in the very practices that are the bellwether of sound security.

Yet, the majority of events analyzed by the Security Response Team for this report are far more ordinary, and many are readily mitigated by patching legacy vulnerabilities and addressing misconfigurations that limit attack paths.

Indeed, even as we see the vulnerability and threat landscape constantly evolving from year to year, we recognize a certain familiarity in the struggles organizations face as they tackle age-old security challenges in new infrastructure. Organizations continue to struggle with protecting, or even defining, the perimeter. Migration to cloud platforms, reliance on managed service providers, software and infrastructure as a service have all changed how organizations must think about and secure the perimeter. Fragmented security solutions and poorly defined security outcomes must be left behind to match the complexity of the modern attack surface.

Defining risk is more important than ever. Beyond counting up the individual vulnerabilities or misconfigurations on their systems, modern security leaders and practitioners must think more holistically about the attack paths that exist within their networks and how they can efficiently disrupt them. We must examine threat actor behavior to understand which attack paths are the most fruitful and leverage these insights to define an effective security strategy. And we must consider the peculiarities of dealing with cloud vulnerabilities, which present unique challenges for organizations seeking to understand their own risk and security posture.

The goal of this report is to help defenders understand the full scope of today's modern attack surface so they can continue to refine their cybersecurity strategies and reduce risk. In this report, we explore:

- The most notable vulnerabilities of the year and how they were used in attack chains, with specific focus on the value of Active Directory to threat actors.
- Risks presented by increased connectivity across information and operational technology.
- The unique challenges of understanding security postures in cloud environments.
- How trust relationships can be exploited by attackers to gain access to sensitive environments.
- How ransomware groups continue to evolve, from double extortion to attacks against critical infrastructure and the supply chain.
- Breach factors and the challenges in analyzing breach data, given the limited information available.
- Details of the key vulnerabilities affecting enterprise software.

Key Stats

21,957
New CVEs Assigned in 2021

1,825
Total Breach Entries*

40B+
Total Records Exposed*

105
Total number of zero-day vulnerabilities

* November 2020 - October 2021

TOP 5 VULNERABILITIES IN 2021

1	2	3	4	5
PROXYLOGON, MICROSOFT EXCHANGE SERVER	**PRINTNIGHTMARE, WINDOWS PRINT SPOOLER**	**VMWARE VSPHERE**	**PULSE CONNECT SECURE**	**ZEROLOGON, WINDOWS NETLOGON PROTOCOL**
CVE-2021-26855	CVE-2021-34527	CVE-2021-21985	CVE-2021-22893	CVE-2020-1472

Key Takeaways

Evolution of the perimeter:
Adoption of cloud solutions, software and infrastructure as a service, and the increasingly complex service provider ecosystem all continue to challenge traditional conceptions of the perimeter. However, traditional perimeter devices like VPNs remain valuable targets for attackers.

Patching problems:
Staying on top of patching assets is difficult enough, but in 2021 it was even more challenging due to incomplete patches, miscommunications from vendors and patch bypasses, making it even harder for defenders to stay on top of securing critical systems.

Majority of zero-days exploited in the wild
83% of zero-day vulnerabilities disclosed in 2021 were exploited in attacks with web browser zero-days accounting for over **30%** of them.

Ongoing risks of interconnection:
Code and library re-use have resulted in vulnerabilities persisting for years across potentially millions of sensitive operational technology (OT) devices. Software libraries and network stacks used commonly amongst OT devices often introduce additional risk when security controls and code audits are not in place.

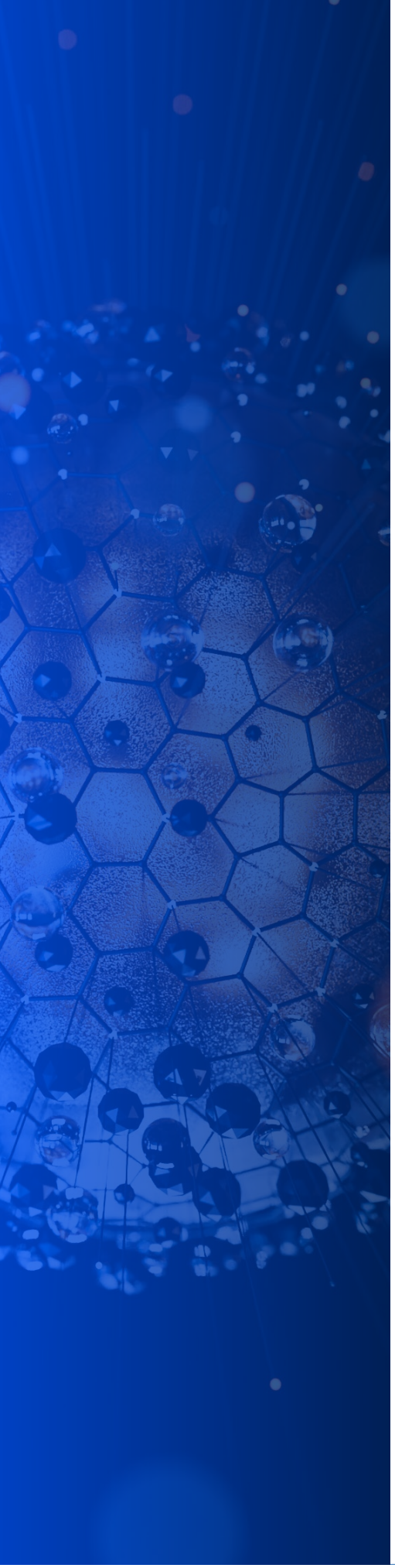
Misconfigurations increase risk:
Cloud and Active Directory (AD) misconfigurations are low hanging fruit for threat actors. Openly accessible cloud databases and overly permissive AD configurations give attackers access to an organization's most sensitive information.

Attackers target AD environments:
Threat groups, particularly ransomware, have increasingly exploited vulnerabilities and misconfigurations in Active Directory.

Surging ransomware attacks:
Ransomware attacks increased in both volume and sophistication. Ransomware groups leveraged zero-days and legacy vulnerabilities alike to target sensitive sectors like healthcare, education and the physical supply chain.

Physical and software supply chains under attack:
Supply chains of all kinds were targeted by diverse threat groups in 2021. Ransomware groups favored physical supply chain disruption as a tactic to extort payment while cyberespionage campaigns exploited the software supply chain to access sensitive data. And **61%** of security leaders reported that their organization was exposed to increased risk related to its expanding supply chain.

Data breaches continue to increase:
Over 2.5 times as many breaches were reported in 2021 than in 2020. Additionally, there was a **78%** increase in the number of records exposed.



Methodology

This report was compiled based on events we've analyzed throughout 2021. We tracked government, vendor and researcher advisories to understand the vulnerability and threat landscapes. Our breach data was compiled by collecting publicly available information from national and local news outlets reporting on data breaches from November 2020 through October 2021. The common vulnerability scoring system (CVSS) scores found throughout the report are derived from the National Institute of Standards and Technology's (NIST) National Vulnerability Database (NVD). In cases where no NVD score is available, scoring is based on the vendor advisory or vulnerability disclosure.

How to use this report

- Disrupt attack paths by identifying and remediating the vulnerabilities and misconfigurations referenced in this report.
- Keep attackers at bay by learning how threat actors are breaching organizations and the tactics they're employing to hold organizations for ransom.
- Protect data by examining some of the common ways data breaches occur and what your organization can do to prevent them from happening.
- Redefine the perimeter by examining how cloud and OT assets are secured and integrated within your organization.
- Broaden your security controls and address AD misconfigurations that attackers continue to target.

Introduction

Throughout the year, Tenable's Security Response Team tracks and reports on vulnerabilities and security incidents, providing guidance to security professionals as they plan their response strategies. We compile those year-long observations and analyze them holistically to better understand the evolution of the threat landscape. These findings provide insight into how organizations should prepare to face the oncoming challenges in 2022. Understanding threat actor behavior can help organizations effectively prioritize security efforts to disrupt attack paths and protect critical systems and assets.

In Section 1, we explore the 2021 vulnerability landscape and the trends that defined it, including:

- Flaws in ubiquitous products like Microsoft Exchange and Windows Print Spooler
- Analysis of the zero-days disclosed and exploited
- The impact of legacy vulnerabilities, particularly those in Secure Socket Layer Virtual Private Networks (SSL VPNs)
- Vulnerabilities and common misconfigurations affecting OT and cloud infrastructure

In Section 2, we explore attacker behavior in the 2021 threat landscape, including:

- Attacks against the software supply chain
- The surge in ransomware attacks against nearly all sectors
- Analysis of the year's data breaches

In Section 3, we provide a detailed list of key vulnerabilities affecting a wide range of vendors, including:

SECTION 1

Vulnerability Landscape

Each year, members of the security community disclose tens of thousands of vulnerabilities in a variety of products used for business. From 2016 to 2021, the number of reported CVEs increased at an average annual growth rate of **28.3%**. The 21,957 CVEs reported in 2021 represent a **19.6%** increase over the 18,358 reported in 2020 and a **241%** increase over the 6,447 disclosed in 2016. The following section explores some key trends in the 2021 vulnerability landscape.

Microsoft Exchange Vulnerabilities

From the beginning of 2021, threat actors targeted vulnerable Microsoft Exchange instances around the world. These threat actors leveraged a host of vulnerabilities in on-premises Exchange disclosed throughout the year. While the specific features of the vulnerabilities differ (full details can be found in Section 3), they are uniquely attractive to attackers because of the ubiquity of Microsoft Exchange in high-value environments.

CVE	Vulnerability Type	CVSSv3
ProxyLogon CVE-2021-26855	Server-Side Request Forgery	9.8
CVE-2021-26857	Insecure Deserialization	7.8
CVE-2021-26858	Arbitrary File Write	7.8
CVE-2021-27065	Arbitrary File Write	7.8
ProxyShell CVE-2021-34473	Remote Code Execution	9.8
CVE-2021-34523	Elevation of Privilege	9.8
CVE-2021-31207	Security Feature Bypass	7.2
CVE-2021-42321	Remote Code Execution	8.8

In March, Microsoft disclosed a state-sponsored cyberespionage campaign exploiting four zero-day vulnerabilities in Microsoft Exchange Server that had begun in January. ESET research later reported that other cyberespionage groups were exploiting this attack chain, specifically calling out CVE-2021-26855, named ProxyLogon. It was eventually revealed that over 60,000 organizations were compromised in these attacks. Over time, ProxyLogon was adopted by non-state-sponsored attackers to distribute cryptominers and ransomware.

According to a joint alert from the Cybersecurity and Infrastructure Security Agency (CISA), Australian Cyber Security Centre (ACSC), United Kingdom's National Cyber Security Centre (NCSC) and Federal Bureau of Investigation (FBI) issued in July, ProxyLogon and its companions were some of the top exploited vulnerabilities by threat groups in the first half of 2021. Attacks against vulnerable servers were so rampant that, in April, the FBI conducted an operation to remotely remove malicious web shells from affected servers.

In August, the ProxyShell attack chain was disclosed at the Black Hat USA and DEF CON security conferences. Like ProxyLogon, ProxyShell was quickly adopted into attack chains by advanced persistent threat (APT) and nation-state groups. According to reports, the LockFile, Conti, BlackByte and Babuk ransomware groups have all adopted this attack chain, as have cryptomining botnets and malicious spam campaigns. Having already been the subject of government warnings, we expect the ProxyShell attack chain will remain among the top exploited vulnerabilities from 2021.

To wrap out the year, Microsoft patched CVE-2021-42321, a post-authentication remote code execution (RCE) in Exchange that was exploited at the Tianfu Cup, a Chinese cybersecurity contest. The Microsoft Threat Intelligence Center also reported limited targeted attacks exploiting this flaw and it was quickly added to CISA's Catalog of Known Exploited Vulnerabilities.

A key reason these vulnerabilities have been utilized heavily by attackers is the widespread use and accessibility of Exchange Servers at organizations around the world and due to their ability to be chained with other vulnerabilities. ProxyLogon and ProxyShell have been chained with several of the vulnerabilities we cover in following sections. For instance, the Black Kingdom ransomware has chained ProxyLogon with a vulnerability in Pulse Connect Secure that was among our Top 5 Vulnerabilities of 2020 (CVE-2019-11510) and the LockFile ransomware has chained ProxyShell with either PetitPotam, a new technology LAN manager (NTLM) relay attack, or Zerologon (CVE-2020-1472) to target AD. AD is a top target, particularly for ransomware. Threat actors seek out attack chains that allow them to pivot from remote attacks into AD takeover.

THE PROXYSHELL ATTACK CHAIN WILL REMAIN AMONG THE TOP EXPLOITED VULNERABILITIES FROM 2021.

Print Spooler

The summer of 2020 saw a flurry of activity so great, we dubbed it "Vulnerability Season." If we continue that naming convention, the summer of 2021 was "Print Spooler Season." From June through October, nearly a dozen vulnerabilities were disclosed in Windows Print Spooler, the Microsoft service that supports all printing functions, including 'print to PDF', in Windows environments.

Attacks targeting Print Spooler are not new though. Over a decade ago, Print Spooler was exploited in the Stuxnet attacks. Much like Microsoft Exchange Server, the ubiquity of the service makes it valuable for attacks but even more so because it is enabled by default in the vast majority of environments, most notably on domain controllers.

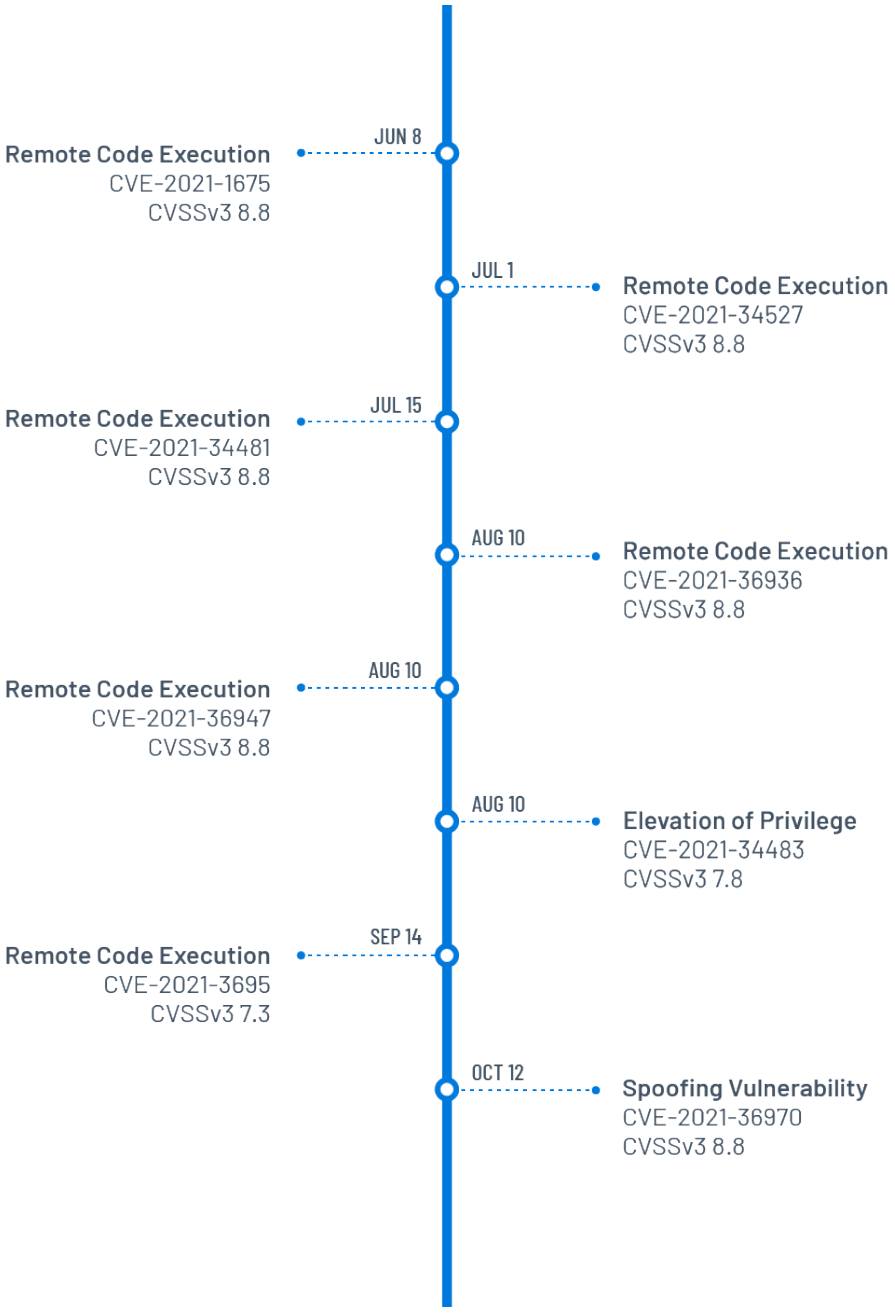
Nearly a dozen vulnerabilities were disclosed and patched in Print Spooler during the summer creating confusion and stress among defenders. This was especially disruptive given the continued necessity of printer functionality in many corporate environments. The confusion began at the end of June when two different research teams published information about CVE-2021-1675. As it turned out, the second proof-of-concept (PoC) release, the one named "PrintNightmare," was a distinct vulnerability which received CVE-2021-34527 and an out-of-band patch. Over the following months, Microsoft released many more updates for Print Spooler and even changed the default behavior of the Point and Print function, which was key to many of the exploits released.

What is PrintNightmare?

While originally the name given to the PoC developed for CVE-2021-34527, PrintNightmare became a catch-all term for vulnerabilities in Print Spooler disclosed in the relevant timeframe by a certain set of researchers.

As with the Exchange vulnerabilities, these Print Spooler flaws have been widely adopted by threat actors. Ransomware groups in particular were attracted to these vulnerabilities due to the high probability that a wide scope of targets would have the service enabled. Magniber and Vice Society ransomware have both leveraged CVE-2021-34527 in their attack chains.

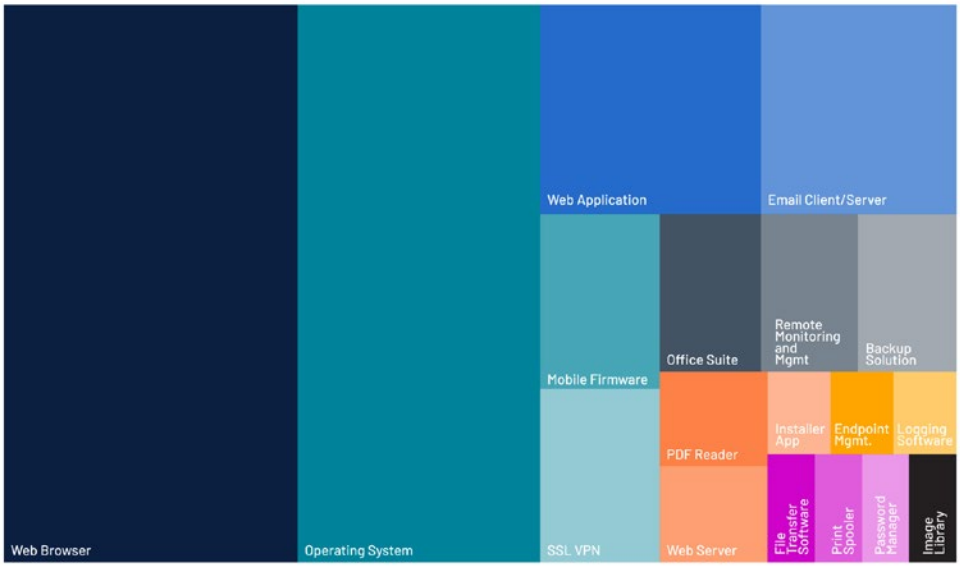
Timeline of Print Spooler Disclosures



Zero-Day Vulnerabilities

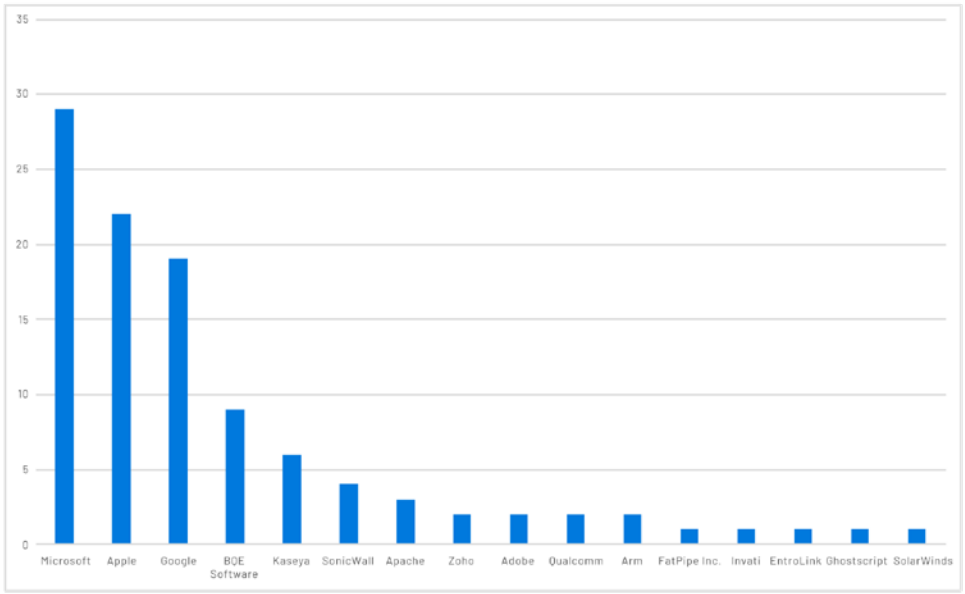
Our analysis of publicly available vendor advisories, news articles and disclosures about zero-day vulnerabilities throughout the year reveals that **105 zero-day** vulnerabilities were disclosed in 2021 across a variety of popular software applications. As we saw last year, browser-related vulnerabilities led the pack, capturing **30.5%** of the market share for zero-days in 2021, a **5.2% decrease** from 2020. Operating systems accounted for **25.7%** of zero-day vulnerabilities identified in 2021, a **2.9% decrease** from 2020. In the chart below, we have broken down the zero-day vulnerabilities by product type and the number of vulnerabilities identified.

2021 Zero-Day Vulnerabilities by Software/Hardware Type



This year, **27.6%** of all zero-day vulnerabilities were found in Microsoft products, followed by Apple with **21%** and Google products at **18.1%**.

2021 Zero-Day Vulnerabilities by Vendors

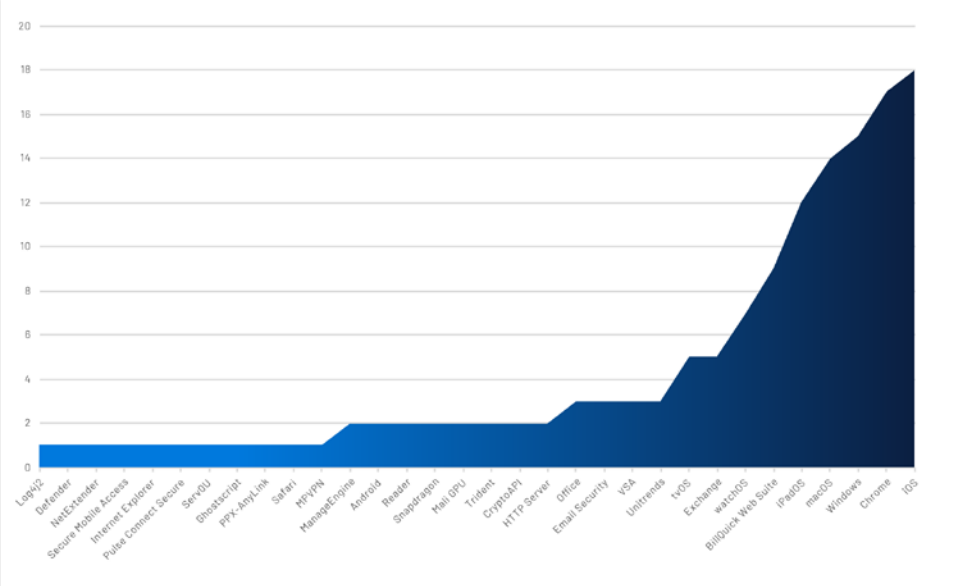


A ZERO-DAY VULNERABILITY IS A FLAW IN SOFTWARE OR HARDWARE THAT IS UNKNOWN TO A VENDOR PRIOR TO ITS PUBLIC DISCLOSURE, OR HAS BEEN PUBLICLY DISCLOSED PRIOR TO A PATCH BEING MADE AVAILABLE.

ZERO-DAY VULNERABILITIES TYPICALLY BECOME MORE PROBLEMATIC FOR MOST ORGANIZATIONS AFTER THEY'VE MADE THE TRANSITION TO LEGACY STATUS.

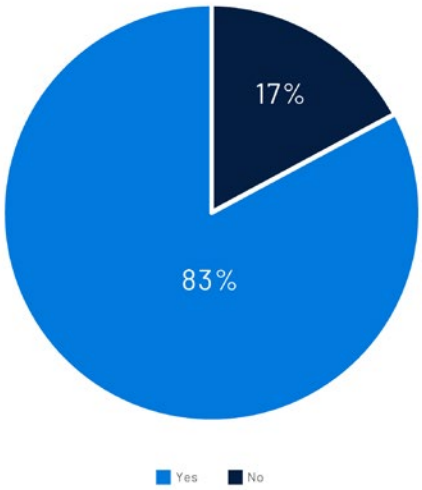
As expected, the bulk of zero-day vulnerabilities originated in products with a large user base. Apple iOS accounted for **12.8%** of all zero-day vulnerabilities identified this year, followed by Google Chrome at **12.1%**. Microsoft Windows-based vulnerabilities accounted for **10.6%** of all those identified.

2021 Zero-Day Vulnerabilities by Products



2021 Zero-Day Vulnerabilities by In-the-Wild Exploitation

Our analysis shows that **83%** of the zero-day vulnerabilities we've tracked in 2021 have been exploited in the wild.



Many of the details surrounding zero-day vulnerabilities are often kept under wraps as vendors focus on providing patches and ensuring users have had ample time to apply said patches.

Zero-day vulnerabilities are primarily leveraged in limited, targeted attacks against a specific set of victims, so the risk to most organizations is minimal at best. That said, the true value of a zero-day vulnerability is often not defined by its exploitation prior to discovery, but by the blog posts and proof-of-concept code published in the weeks and months after disclosure . Zero-day vulnerabilities typically become more problematic for most organizations after they've made the transition to legacy status, particularly if an organization has not yet applied available patches before widespread exploitation begins.

One zero-day that simultaneously counters and supports what we know about zero-day vulnerabilities is CVE-2021-44228, Log4Shell. It is ubiquitous enough to have immediately been a concern for huge swaths of the internet-connected world and will assuredly have a long tail as vendors and organizations alike try to determine where they have either implemented the vulnerable framework or deployed a product that does, and remediate all instances. Attackers were exploiting Log4Shell **as early as December 1**, more than a week before it became a publicly known zero-day. After public disclosure, attackers were off to the races. **Botnets** and **ransomware** led the charge in adopting the exploit, as they so often do, and **nation-states** soon joined the fray.

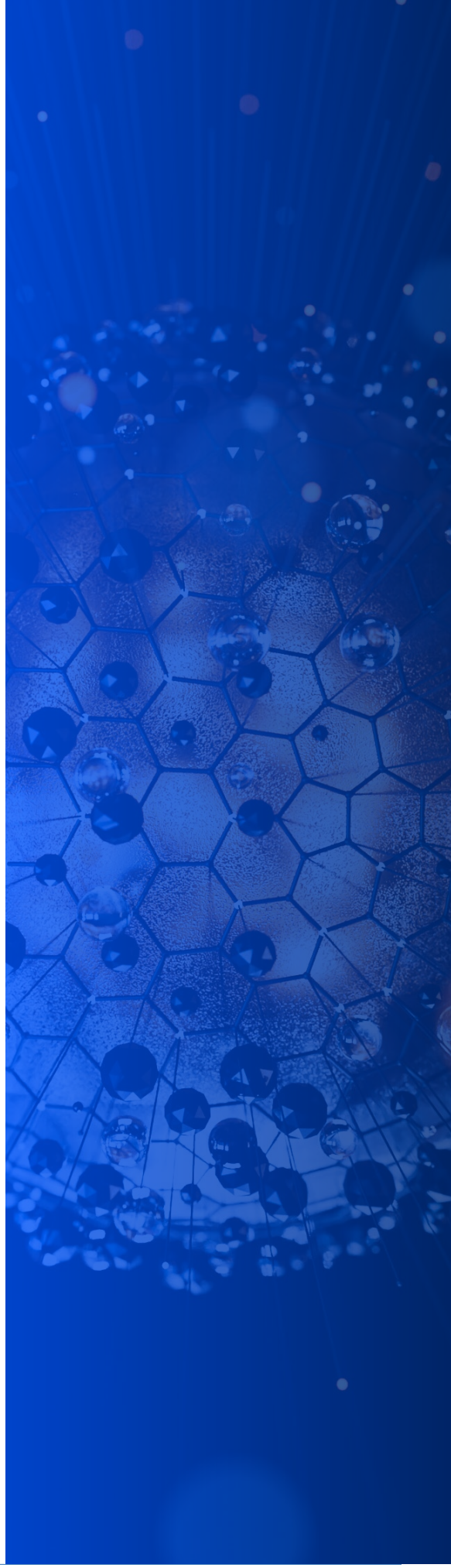
Still VPNs

In the 2020 Threat Landscape Retrospective, we highlighted the risks posed by legacy vulnerabilities. One class of legacy vulnerabilities in particular, secure socket layer SSL VPN flaws, made up three of our top five vulnerabilities from 2020:

- **CVE-2018-13379:**
  Fortinet FortiOS SSL VPN Web Portal Information Disclosure
- **CVE-2019-11510:**
  Pulse Connect Secure Arbitrary File Disclosure
- **CVE-2019-19781:**
  Citrix Application Delivery Controller (ADC) and Gateway Directory Traversal

Even though these three flaws were patched between 2019 and early 2020, they were some of the most exploited vulnerabilities throughout 2020. They were featured in **several government alerts** from U.S. agencies like CISA, the NSA and the FBI, highlighting their use by APT and ransomware groups.

Our concern was that, as with most legacy vulnerabilities, these flaws would be forgotten and left unpatched amidst the plethora of vulnerabilities disclosed and exploited in 2021. In fact, we published a **blog post in August 2021** stressing the importance for organizations to patch their SSL VPNs, as we continued to see these flaws being exploited by attackers in the wild. In 2022, we expect VPN vulnerabilities to continue wreaking considerable havoc against organizations. Outside of these three vulnerabilities, attackers utilized other legacy flaws, as well as new vulnerabilities in SSL VPNs, throughout 2021.



UNPATCHED SSL VPNS ARE AN IDEAL ENTRY POINT FOR ATTACKERS TO GAIN A FOOTHOLD IN A NETWORK TO PERFORM CYBERESPIONAGE, EXFILTRATE SENSITIVE AND PROPRIETARY INFORMATION AS WELL AS ENCRYPT NETWORKS AND HOLD THEM FOR RANSOM.

In January, SonicWall was targeted by "highly sophisticated threat actors" that breached its internal systems. In late January, NCC Group identified a candidate for the breach and in February, SonicWall published an advisory for CVE-2021-20016, a zero-day vulnerability in its Secure Mobile Access SSL VPN.

In April, Ivanti, which acquired Pulse Secure in 2020, published an out-of-cycle security advisory for CVE-2021-22893, an authentication bypass zero-day vulnerability in Pulse Connect Secure that was being exploited by attackers in the wild to target government agencies. In addition to this newly disclosed flaw, Ivanti also placed emphasis on other legacy vulnerabilities being leveraged in the bulk of attacker-related activity, including: CVE-2019-11510, CVE-2020-8243, a code injection vulnerability and CVE-2020-8260, an unrestricted file upload vulnerability.

In July, CVE-2019-19781, a critical vulnerability in the Citrix ADC and Gateway was identified as the No. 1 most-exploited vulnerability in 2020 in a joint advisory issued by CISA, the ACSC, the United Kingdom's NCSC and FBI. In January 2021, this vulnerability was used by attackers to breach the U.S. Census Bureau systems in January.

Unpatched SSL VPNs are an ideal entry point for attackers to gain a foothold in a network to perform cyberespionage, exfiltrate sensitive and proprietary information as well as encrypt networks and hold them for ransom. As part of a post-mortem into a ransomware attack, Capcom confirmed that attackers managed to gain access to its network by targeting an old VPN backup device. Even if the attackers don't leverage this access, they can sell it to the highest bidder, as we saw when attackers exploited a Fortinet FortiOS SSL VPN vulnerability and leaked 500,000 credentials.

The NSA and CISA published an information sheet in September on how to select and harden VPNs through a variety of measures, including the timely application of patches that address critical vulnerabilities like the ones referenced above.

As we grapple with the paradigm shift in the workforce, whether it is a hybrid or fully remote strategy, VPNs will continue to remain a popular target for cybercriminals. Therefore, it is paramount for organizations to protect their perimeters by identifying these assets and ensuring they receive regular security updates.

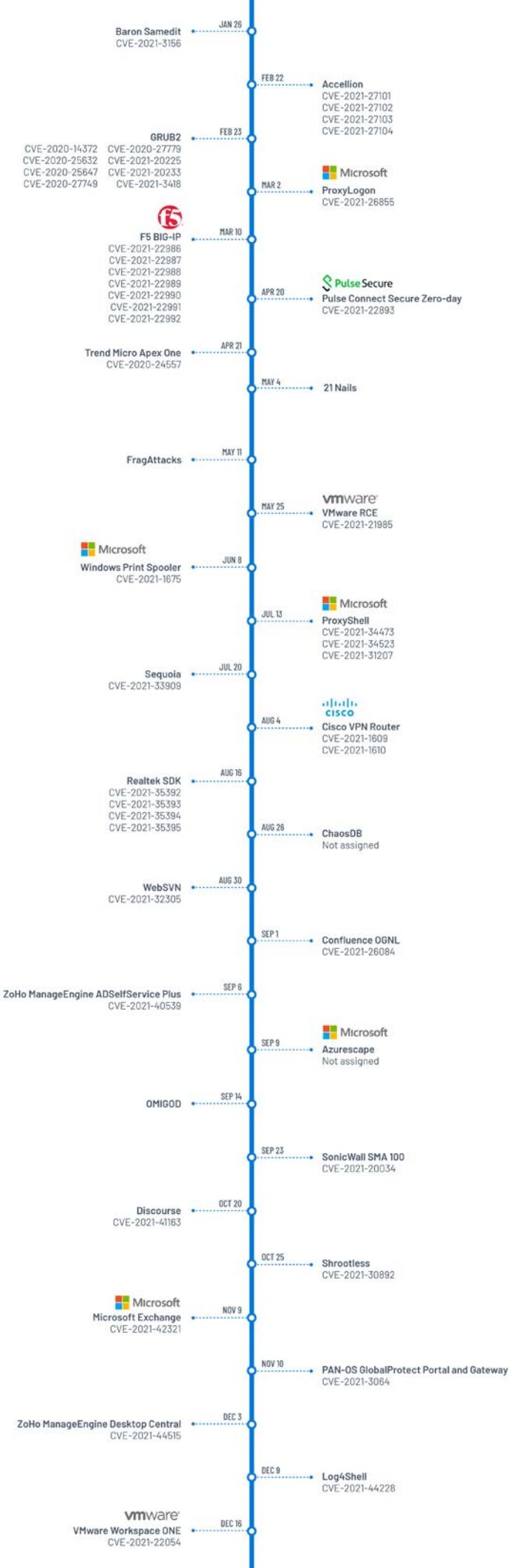
Other Vulnerabilities of Interest in 2021

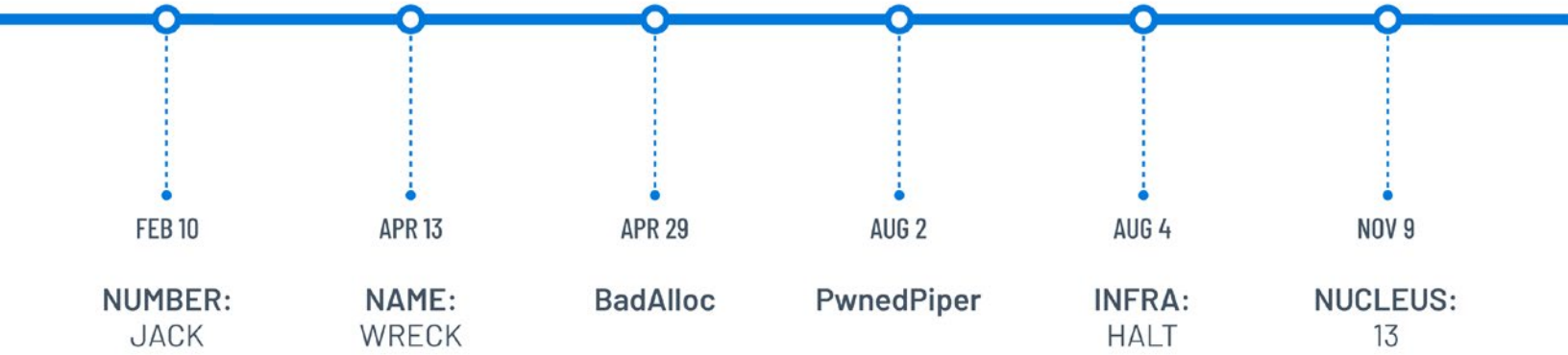
Named vulnerabilities and attack chains dominated the news cycle while having varied real-world effects on organizations. As is always the case, many unnamed vulnerabilities proved much more effective than their named counterparts. Perimeter devices like SSL VPNs, Microsoft and Apple products, cloud solutions and operational technologies were all among notable targets for these attacks.

Governments name the most-exploited flaws

The joint cybersecurity advisory from CISA, the FBI, ACSC and NCSC that listed the most exploited vulnerabilities in 2020 and the first half of 2021 stated that threat actors have been prioritizing "perimeter-type devices" in their attacks. Microsoft Exchange, Accellion, Pulse Secure and Fortinet SSL VPNs were the most exploited for the first half of the year and are covered in other sections of this report. The Accellion incident at the beginning of the year, wherein threat actors leveraged a vulnerability in the File Transfer Appliance, had a far-reaching impact. Dozens of organizations have disclosed data breaches linked to the four zero-days patched by Accellion.

Another top exploited vulnerability in 2021 was CVE-2021-21985, a RCE in VMware vCenter Server. Patched at the end of May, mass scanning, likely by threat actors, for CVE-2021-21985 was reported on June 3, the same day a working PoC was published. In September, VMware patched CVE-2021-22005, an arbitrary file upload vulnerability that was quickly adopted by threat actors. In October, CISA included it in the "Catalog of Known Exploited Vulnerabilities" released alongside Binding Operational Directive (BOD) 22-01. The BOD lists vulnerabilities that represent "significant risk to the federal enterprise." It also calls for aggressive remediation of all the vulnerabilities listed in the catalog.





Operational Technology

In the wake of major attacks on critical infrastructure in 2021, concerns surrounding the security of OT environments have never been higher. In May, the White House released Executive Order (EO) 14028, "Improving the Nation's Cybersecurity." The executive order outlines policies and steps to ensure the federal government and private sector work hand-in-hand to prioritize and modernize cybersecurity strategy. Recognizing the importance of OT, the executive order mentions the importance of protecting these systems used in critical industries.

While doomsday scenarios and predictions are made each year, 2021 proved that information technology (IT) and OT environments are in attackers' crosshairs. In the early hours of the Colonial Pipeline incident, fears were high around the impact the ransomware attack may have had on Colonial's OT environment. While we later learned none of the OT environment was impacted, the incident highlighted the importance of securing organizations that are critical to the supply chain. As the prevalence of connected devices grows, researchers continue to examine OT security and risks by focusing on the underlying protocol stacks utilized by these devices.

Over the past few years, there have been a number of research efforts to highlight the flaws within OT/internet of things (IoT) devices, including URGENT/11, Ripple20 and AMNESIA:33.

Since January, researchers have publicly disclosed over 80 vulnerabilities across several libraries and software development kits (SDKs) found in billions of devices across the globe.

Date	Vulnerability Campaign	Number of Vulnerabilities Identified
February 10	NUMBER:JACK	9
April 13	NUMBER:WRECK	9
April 29	BadAlloc	27
August 2	PwnedPiper	9
August 4	INFRA:HALT	14
November 9	NUCLEUS:13	13

As part of Project Memoria, Forescout Research Labs began researching Transmission Control Protocol/Internet Protocol (TCP/IP) stacks used by various devices. As the backbone of interconnected network devices, TCP/IP is a foundational set of communications protocols and an ideal target for exploration. As part of its research, Forescout released four pieces of research this year. Starting with NUMBER:JACK, the research focuses on TCP/IP stack security and explores nine vulnerabilities affecting multiple TCP/IP stacks. Less than two months later, Forescout released NAME:WRECK, a new set of nine vulnerabilities found across four TCP/IP stacks. The focus of this research was Domain Name System (DNS) vulnerabilities. INFRA:HALT, a joint research effort from Forescout and JFrog Security Research focused on the NicheStack TCP/IP stack and contained 14 new vulnerabilities. NicheStack is used in OT and industrial control systems (ICS) devices found in critical infrastructure and used by some of the biggest OT device manufacturers. In November, Forescout released NUCLEUS:13, a set of 13 vulnerabilities in the Nucleus TCP/IP stack. Nucleus NET is the TCP/IP stack of the Siemens-owned Nucleus real-time operating systems (RTOS), which is reportedly used in a staggering 3 billion devices.

In April, Microsoft's Section 52, the Azure Defender for IoT security research group, announced a set of 27 critical memory allocation vulnerabilities dubbed BadAlloc. These vulnerabilities were found in a range of RTOS, SDKs and C standard library (libc) implementations used in a wide variety of devices.

Armis researchers disclosed PwnedPiper in August, a set of nine critical vulnerabilities in the Translogic pneumatic tube system (PTS) used to transfer materials in thousands of hospitals. These nine vulnerabilities can be exploited to take control of the PTS system to physically manipulate sensitive materials, like blood samples, as well as taking control of the paths to redirect a carrier to another path. In a real-world scenario, one could imagine the disastrous effects an attack like this would have for patients in need of urgent care.

As we reflect on the assortment of vulnerabilities found within the libraries, SDKs and RTOSes within billions of devices across the world, we are reminded of the complexities in securing these devices. A common theme from many of these disclosures is the use of insecure protocols such as file transfer protocol and telnet. While these protocols have served a purpose in years past, they present unnecessary risk to organizations that may not even be aware the services are running. With the widespread use and re-use of software libraries and RTOS across numerous devices and manufacturers, patch management and asset enumeration remain difficult problems for most organizations. In some cases, mitigations and network segmentation may be the only viable options for devices that may no longer be manufactured or supported by vendors.

We are now seeing the OT landscape struggle with some of the security concerns that plagued desktops in the early 2000s. With a holistic approach to security, organizations can make strides to protect themselves. This includes examining which devices are on the network and which controls are in place to prevent unnecessary network access to sensitive devices. We must recognize the importance these devices have in our everyday lives and take appropriate steps to secure them.

65% OF SECURITY LEADERS SURVEYED BY FORRESTER CONSULTING ON BEHALF OF TENABLE ATTRIBUTED CYBERATTACKS AT THEIR ORGANIZATIONS TO COMPROMISES AT THIRD-PARTY SOFTWARE VENDORS.

42%

of organizations moved business-critical function to the cloud

36%

moved non-business-critical functions

*Source: "The Future of Cybersecurity in the New World of Work," a commissioned study of 426 security leaders, 422 business executives and 479 remote workers conducted by Forrester Consulting on behalf of Tenable, September 2021.

Cloud

Cloud adoption has been on the rise, accelerating as organizations have adapted their strategies due to the COVID-19 pandemic. In fact, a commissioned study conducted by Forrester Consulting on behalf of Tenable revealed that **42%** of organizations moved business-critical functions to the cloud, while **36%** moved non-business-critical functions.

As more data and business operations move to the cloud, organizations must prioritize the proper implementation of security controls. Section 3 of EO 14028, "Improving the Nation's Cybersecurity," focuses on modernizing federal government cybersecurity and acknowledges that cloud adoption should be accelerated while implementing security best practices. In response to this, CISA has developed the Cloud Security Technical Reference Architecture. This guide aims to provide recommendations for cloud migration and data protection leveraging cloud security posture management. With significant investment in cloud infrastructure from the U.S. government, it's clear that cloud usage will continue to increase.

Cloud vulnerabilities are a peculiar category because they are typically fixed by the cloud providers, often without any CVE identifier, changelog or notices to end users. This presents a unique challenge for organizations understanding their own risk and security posture and potentially introduces new vulnerabilities and attack paths with feature updates from cloud vendors. Because of this, research into cloud security continues to remain paramount to providing a more secure ecosystem.

Throughout the year, research teams and individuals worked to discover and disclose vulnerabilities in cloud solutions. According to reports from vendors, most of these flaws were disclosed and fixed before they could be exploited by threat actors.

In August, the Wiz Research Team disclosed ChaosDB, a vulnerability in Microsoft's Azure cloud platform. Microsoft reportedly mitigated the issue within 48 hours of the disclosure and did not issue a CVE identifier for the vulnerability. Microsoft notified multiple Cosmos DB customers to report potential breaches, despite claiming it observed no evidence of exploitation in the wild. While the flaw is no longer present in the platform, this example demonstrates how a vulnerability in a cloud service can go undetected, potentially for months, threatening the security of thousands of organizations.

In September, Palo Alto Networks' Unit 42 Research team disclosed Azurescape, a discovery made through research into Azure Container Instances. This was a significant finding, as no user should be able to break out of their own environment and access and run code on another user's environment. Fortunately the issue was patched by Microsoft shortly after it was reported by Unit 42 and, at the time the disclosure was made, there was no evidence that this flaw had been abused.

In the same month, on September 14, researchers from the Wiz Research Team disclosed **OMIGOD**, four vulnerabilities in Microsoft Azure's Open Management Infrastructure (OMI). Microsoft released a patch for OMI to address the four vulnerabilities on August 11, however the flaws were not disclosed to the public until the **September Patch Tuesday** release. Within only a few days of the disclosure, exploitation attempts of the most critical of the four vulnerabilities, CVE-2021-38647, were observed in the wild. Users that had automatic updates enabled were protected by the OMI patch, however those that didn't remained at risk. Microsoft released a **blog post** on September 16 advising on how to manually update OMI and provided guidance on checking for evidence of exploitation.

In December, researchers from **SentinelOne disclosed** multiple vulnerabilities in a third-party library used by multiple cloud services including Amazon Workspaces, Accops HyWorks and NoMachine. The vulnerabilities were found in Eltima SDK, a library that provides USB over ethernet. This library allows users to connect local USB devices to their remote desktop. As discussed in a prior section above, code and library reuse can result in inherited vulnerabilities and have a wide impact on downstream users. In this case, the library was found to be in use by several cloud providers, but the researchers caution that, because of Eltima SDK's widespread use, other cloud providers may also be impacted. From this research, 27 CVEs were identified and reported to known affected vendors.

As more organizations adopt cloud solutions, vulnerabilities will remain top of mind. However cloud misconfigurations, like unsecured storage buckets, passwords or encryption keys in open repositories, improper access controls and others that result in the **compromise of sensitive data**, pose a larger threat to most organizations. While each cloud provider offers its own best practices and default policy options, it's imperative that organizations take the time to **properly assess** their cloud environments and ensure that such misconfiguration issues are not overlooked. Insecure cloud instances are a valuable target for attackers and have been abused to **mine cryptocurrency** and conduct phishing attacks. There's no doubt cloud is here to stay, bringing with it a new set of challenges in securing an organization and its data.

SECTION 2

Threat Landscape

Beyond the vulnerabilities and security issues affecting organizations throughout the year, it is crucial to examine attacker behavior. To what end were threat groups exploiting the flaws we just examined? The threat landscape is constantly evolving, defender behavior should adapt to match attacker priorities.

Supply Chain

The major news that closed out 2020 was the supply chain attack via SolarWinds. Shortly into 2021, it became obvious that supply chain attacks would be a key feature of the threat landscape. While attackers also leveled attacks on the physical supply chain, this section examines flaws within the software supply chain on which organizations rely to develop and defend their systems, products and customers.

As we closed out 2020, information about the sophisticated cyberespionage campaign achieved via the SolarWinds Orion platform was just coming to light. The nation-state actors, named Nobelium by Microsoft and linked to Russia's foreign intelligence service (SVR), were able to compromise the update protocol for the SolarWinds Orion platform and distribute malware to public and private organizations. The security firm FireEye, a SolarWinds customer, discovered the malicious code and raised the alarm. Several additional vulnerabilities and malware components were discovered in relation to this campaign. A separate zero-day was disclosed in SolarWinds Serv-U Managed File Transfer in July and has been adopted by Clop ransomware.

Beginning in January, a different threat actor breached Codecov — a code coverage tool for application testing — and extracted credentials, keys and tokens from Codecov customers. The unnamed threat actor compromised the Codecov Bash Uploader, which is used to detect and upload reports to Codecov, using stolen credentials from a misconfigured Docker image. They introduced a single line of code that redirected environment variables to an attacker-controlled server. Like SolarWinds, this supply chain compromise was initially reported to Codecov by one of its customers.

In the summer of 2021, another similar supply chain incident affected managed service providers using Kaseya Virtual System Administrator (VSA), a remote monitoring and management software from Kaseya Limited. Rather than cyberespionage, this was a large-scale ransomware campaign leveraging multiple zero-days. In November, a Ukrainian citizen with links to the REvil ransomware group was charged for orchestrating this campaign.

The Nobelium threat group has continued to target supply chains, attempting to compromise targets via resellers and service providers. These incidents also often put organizations on the radar of other attackers. Threat actors have exploited new zero-days in products from both SolarWinds and Kaseya since their supply chain incidents were disclosed.

IT IS NOT JUST ABOUT REMEDIATING VULNERABILITIES IN PRODUCTS YOUR ORGANIZATION DEPLOYS BUT ROUTINELY EVALUATING THE TRUST RELATIONSHIPS WITHIN YOUR ENVIRONMENT AND HOW THEY MIGHT BE EXPLOITED.

These attacks are a reminder that highly motivated attackers will seek diverse ways to compromise organizations. It is not just about remediating vulnerabilities in the products your organization deploys but routinely evaluating the trust relationships within your environment and how they might be exploited. In fact, **65%** of security leaders surveyed by Forrester Consulting on behalf of Tenable attributed cyberattacks at their organizations to compromises at third-party software vendors.

While these incidents are among the most noteworthy from 2021, many others occurred on a smaller scale. Password managers, closed-circuit television cameras and smartphones have all been targets.

Threat actors also compromised open source libraries and repositories to introduce backdoors and cryptominers. The Python Packaging Index, RubyGems, PHP and multiple Node Package Manager (npm) repositories have all been exploited by attackers to compromise a variety of organizations. Security researchers have also examined these backend dependencies and found additional vulnerabilities in the Composer PHP project, GoCD and npm packages which have been fixed by the maintainers of these open source projects. These compromises underscore the risks associated with implementing third-party code into trusted environments and the importance of auditing and mitigating these dependencies regularly.

WITH THE WIDESPREAD USE AND RE-USE OF SOFTWARE LIBRARIES AND RTOS ACROSS NUMEROUS DEVICES AND MANUFACTURERS, PATCH MANAGEMENT AND ASSET ENUMERATION REMAIN DIFFICULT PROBLEMS FOR MOST ORGANIZATIONS.

RANSOMWARE IS MALICIOUS SOFTWARE (OR MALWARE) DESIGNED TO ENCRYPT FILES ON SYSTEMS, HOLDING ORGANIZATIONS HOSTAGE UNLESS A RANSOM DEMAND HAS BEEN PAID.

Ransomware

In 2020, the ransomware landscape was defined by an approach known as double extortion, which was pioneered by the Maze ransomware group at the end of 2019. Whereas the first step of extortion is the encryption of files, the second is the theft of files from a network with the intention of publishing the stolen files if the ransom is not paid. These stolen files are teased on the dark web on websites called leak sites. These leak sites contain a list of victims that have either not engaged in negotiations or where negotiations fell apart. In 2021, double extortion became the linchpin of most ransomware groups and a key factor in the record breaking profits for ransomware operators.

Ransomware attacks on critical infrastructure

The most notable ransomware attack in 2021 happened in May, when the Colonial Pipeline Company, the largest pipeline system in the United States, discovered it was the victim of a ransomware attack linked to the DarkSide ransomware group. As Colonial looked to contain the incident, it halted pipeline operations. This led to panic, which drove consumers to wait in long lines while gas prices and the fear of shortages rose. Despite containing the incident, Colonial paid a ransom demand of nearly $5 million dollars. As for how the attackers breached Colonial's network, its CEO testified before the United States Senate that it was due to a legacy VPN account that lacked multifactor authentication and had not been decommissioned.

JBS, one of the world's largest meat suppliers, also confirmed it was the victim of a ransomware attack at the end of May that was attributed to the REvil ransomware group. As part of the Food and Agriculture sector, JBS is considered critical infrastructure. Similar to the attack against Colonial, JBS had to suspend affected systems, which resulted in operational impact for the organization. Ultimately, JBS also paid the ransom demand of $11 million dollars.

In September, ransomware attacks struck two agricultural supply cooperatives, NEW Cooperative and Crystal Valley. The NEW Cooperative attack was linked to the BlackMatter ransomware group, which demanded a $5.9 million dollar ransom.

Ransomware attacks against critical infrastructure could potentially have a significant impact, especially when operations, such as petroleum pipelines or food processing plants, are shut down. Threat actors rely on these potential disruptions to incentivize organizations to pay the ransom.

Healthcare is the top sector targeted by ransomware groups

Our analysis of breach data for 2021 reveals that ransomware attacks accounted for **24.7%** of healthcare breaches. With the Health Insurance Portability and Accountability Act (HIPAA), entities that fall under the purview of the U.S. Department of Health and Human Services are bound by a data breach notification rule that warrants such entities to report the breach or exposure of unsecured protected health information. With ransomware groups finding massive success in their double extortion tactic, it becomes clear why healthcare would be the top sector targeted by such groups.

One of the most notable healthcare breaches linked to ransomware was conducted by the Conti ransomware group, which crippled Ireland's Health Service Executive in May. A study conducted by Philips and CyberMDX, "Perspectives in Healthcare Security Report," found that close to half of United States Hospitals were shut down due to ransomware attacks, either as a direct result of the attack or to proactively shut down their networks to prevent further infection.

Ransomware groups come and go, but affiliates always remain

Throughout 2021, prominent ransomware groups came and went, either as a result of law enforcement action or self-directed shutdowns. The groups often come back rebranded, like the DarkSide ransomware group returning as BlackMatter after the Colonial Pipeline incident, while others may go on a temporary hiatus to enjoy the summer months, as REvil did after the Kaseya ransomware attacks. What remains, however, are affiliates. Most modern ransomware groups operate a ransomware-as-a-service (RaaS) model.

Affiliates are the engine driving most ransomware attacks today. They are the ones responsible for finding their way into targeted networks. So while ransomware groups may come and go, the affiliates have no allegiance to one ransomware group, often partnering with several.

Legacy vulnerabilities and emerging flaws gain favor with affiliates and ransomware groups

As we've discussed throughout this report, VPN vulnerabilities have been popular across the threat landscape and, in 2021, they were extremely favored with ransomware groups. VPNs are just one of the entry points for an attacker to gain access to a network, which is why we saw ransomware affiliates leveraging the legacy VPN vulnerabilities in Citrix, Fortinet and Pulse Secure.

In addition to these legacy flaws, attackers used zero-days in SonicWall (CVE-2021-20016) and Kaseya (CVE-2021-30116) to gain entry into targeted networks to deploy ransomware, or in the case of the Accellion flaws (CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, CVE-2021-27104), to bypass deploying ransomware and instead exfiltrate sensitive files to post on a leak website.

In August, a playbook for affiliates of the Conti ransomware was leaked, revealing that Conti guides its affiliates to use flaws like Zerologon (CVE-2020-1472), PrintNightmare (CVE-2021-1675, CVE-2021-34527) and EternalBlue (CVE-2017-0143, CVE-2017-0148) during their attacks.

Ransomware affiliates leverage a variety of tactics to breach organizations, including phishing, malware, password reuse and brute-forcing RDP connections. While vulnerabilities aren't the only way ransomware affiliates perform their attacks, they're certainly one of the key tools in their toolboxes to break into targeted networks.

RANSOMWARE-AS-A-SERVICE IS OFFERED BY RANSOMWARE GROUPS AND GIVES AFFILIATES — CYBERCRIMINALS LOOKING TO PARTNER WITH RAAS GROUPS — ACCESS TO RANSOMWARE THAT IS READY TO BE DEPLOYED, AS WELL AS A PLAYBOOK TO HELP GUIDE THEIR ATTACKS. RAAS GROUPS TAKE A SMALL CUT OF RANSOM DEMANDS, PROVIDING THE BULK OF THE PROFITS TO AFFILIATES.

Breaches

Tenable's SRT continuously monitors the threat landscape to stay informed of the latest cybersecurity news and events. As part of our monitoring efforts, we digest breach reports daily in an effort to understand what leads to these breaches. For this retrospective, our analysis covers **1,825 breach events** spanning from November 1, 2020 to October 31, 2021. This analysis explores the data to understand breach trends, such as impacted industries and the root causes, over a 12-month time span.

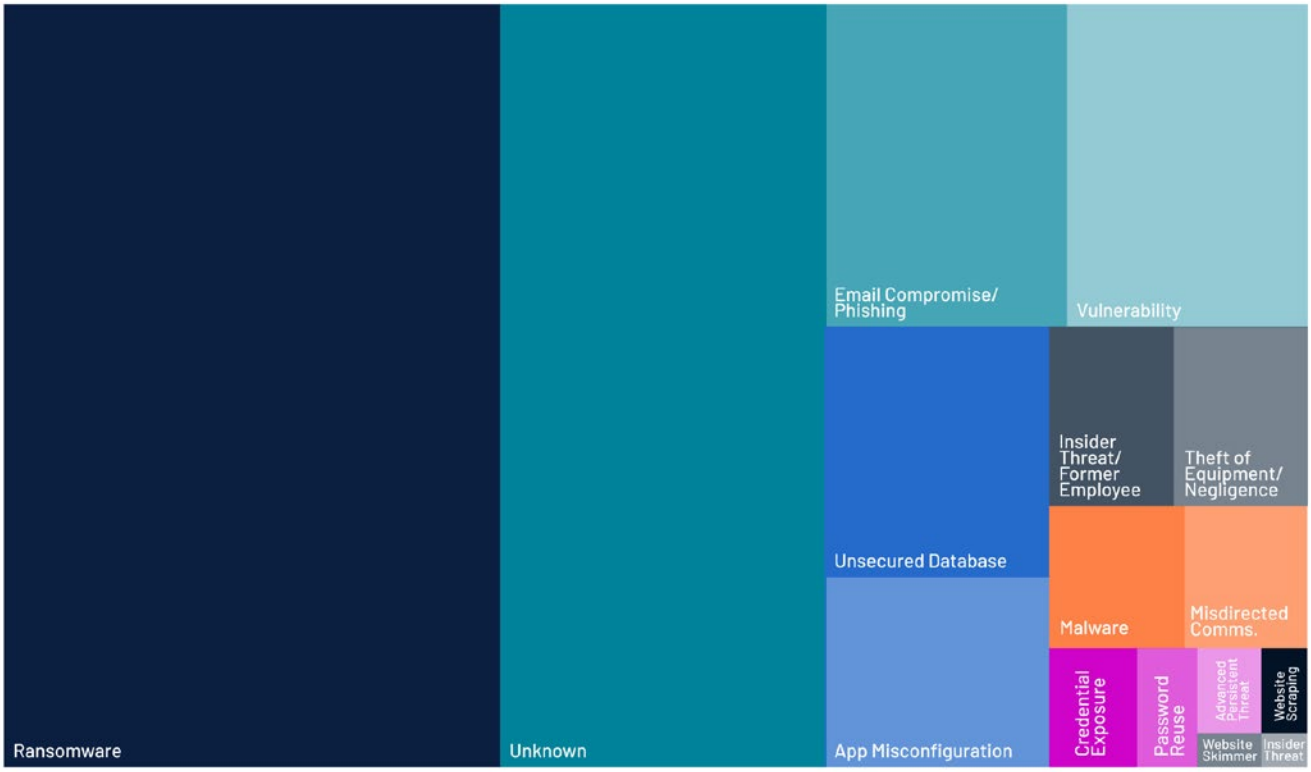
Our list is a best effort and is not intended to be fully exhaustive of all the breaches reported throughout this time period. Based on our past examination of breach data, we know that disclosures may not be made public until months to years after the incident. Additionally, as reporting requirements vary across multiple industries and geographic locations, we must also acknowledge that some industries and locations have no reporting requirements or central authority for reporting, which makes obtaining a comprehensive global view of the breaches that occurred over this time period nearly impossible for anyone attempting to aggregate this data.

Of the 1,825 breach notices we analyzed, we found that over **40 billion (40,417,167,937)** total records were exposed. While this is an incredible number, **87%** of the breach disclosures we analyzed did not include any information on the number of records exposed, meaning this figure is likely much higher.

The amount of data stolen was reported in only a limited number of events. Our analysis reveals that over **260 terabytes** were stolen as a result of these data breaches. In addition, some sources made a distinction between user records and files, documents or emails. The sum of this data is over **1.8 billion files, documents or emails**.

As we continued our data analysis, we looked to answer how many times data breaches were tied to a specific root cause, such as a vulnerability being exploited or a ransomware group. As anyone observing the current threat landscape can attest, ransomware has had monumental impact on organizations in 2021, as approximately **38%** of all breaches analyzed were the result of a ransomware attack. This is up from **35%** in 2020. Dozens of groups, like REvil, Conti, DarkSide and more, dominated the headlines and continued to wreak havoc across a wide range of industries.

2021 Breaches by Root Cause

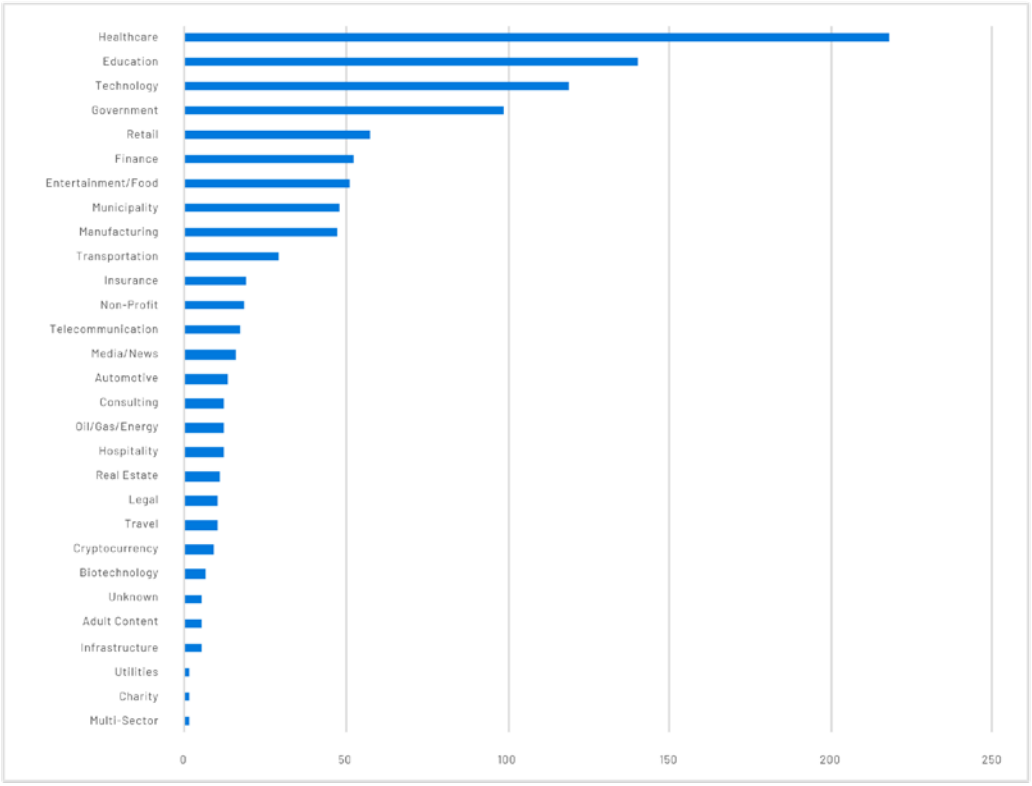


A quarter of the data breaches (**25.7%**) analyzed in 2021 had an unknown root cause, up slightly from **24.5%** in 2020. Unfortunately many organizations do not include information on the source of the breach, which leaves the affected parties with more questions than answers. Because some industries lack any reporting requirements at all, we are likely to continue to be in the dark on most breach notices.

In Section 1 of the report, we discussed how cloud misconfigurations are a concern for organizations as they move more operations and data into cloud environments. From our analysis, **6%** of breaches were the result of unsecured cloud databases. Unsecured cloud storage such as Amazon Web Services (AWS) S3 Buckets and Google Cloud Platform (GCP) buckets, unsecured Elasticsearch databases and unsecured Azure blobs have left millions of records publicly accessible. Simple cloud misconfigurations have exposed data for countless individuals and could have major financial implications for an affected company.

SIMPLE CLOUD MISCONFIGURATIONS HAVE EXPOSED DATA FOR COUNTLESS INDIVIDUALS AND COULD HAVE MAJOR FINANCIAL IMPLICATIONS FOR AN AFFECTED COMPANY.

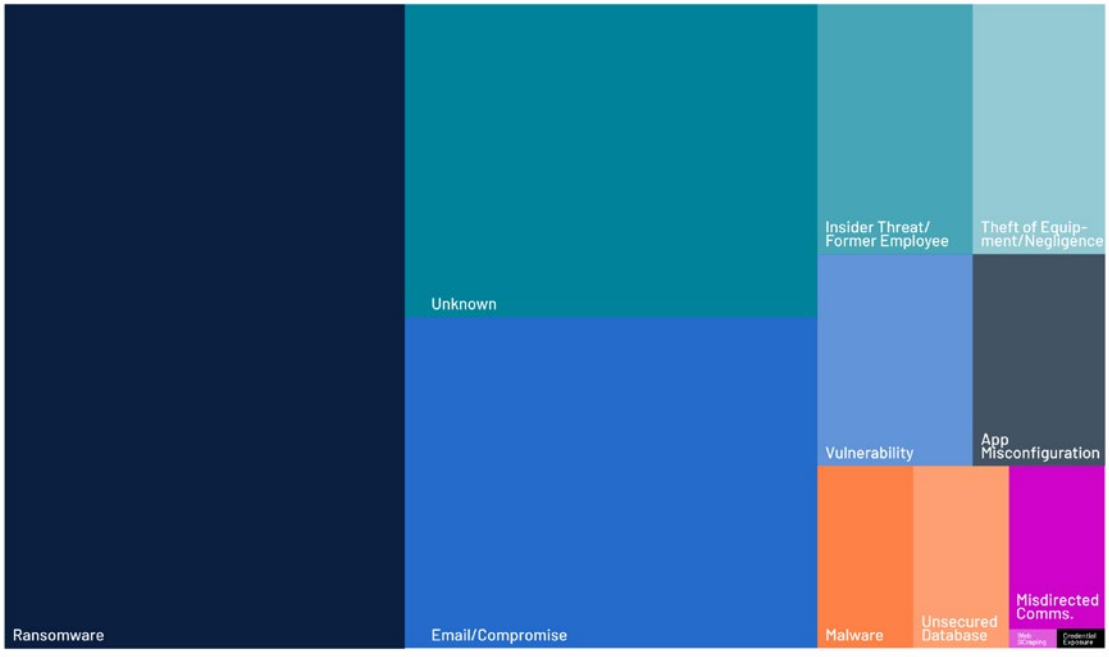
2021 Breaches by Industry



This year's breaches may seem like deja vu, because the same most-targeted industries from 2020, healthcare and education, remained firmly at the top.

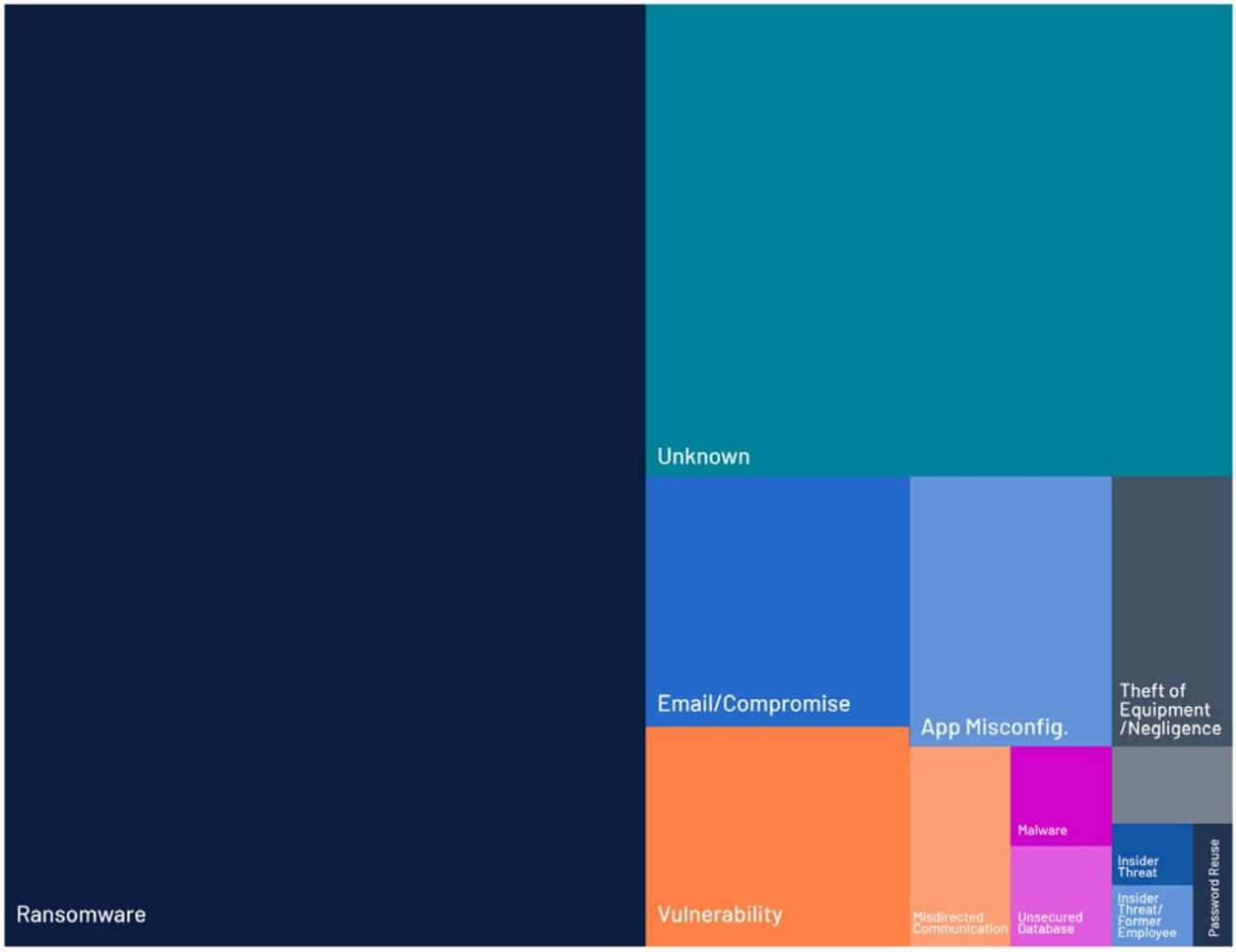
Over **24%** of the breaches analyzed were attributed to the healthcare industry. Hospitals, doctors' offices, billing companies, dentists, therapists and more were impacted by a variety of threats. An incredible **36.2%** of healthcare breaches were caused by ransomware attackers while email compromise and phishing attacks accounted for nearly **19%**.

2021 Healthcare Breaches by Root Cause



Nearly **13%** of breaches were linked to the education sector. Students, educators and parents were impacted by these breaches through canceled classes and inaccessible learning platforms. With thousands of students to serve and a growing IT infrastructure, educational institutions face an uphill battle protecting and securing devices. A staggering **52%** of breaches in the education sector were the result of ransomware attacks. While it's not clear if ransomware groups actively set out to target education facilities, or if this is a result of opportunistic activity targeting easy to find vulnerable devices, this is a worrisome trend.

2021 Education Breaches by Root Cause



As organizations continue to collect troves of data, often out of necessity and in some cases indirectly collected from use of service, the stakes grow higher for the stewards of such data to properly store and secure all they collect. Ransomware groups, vulnerabilities and misconfigurations are just a few of the threats organizations face today — and these threats will continue to pose a risk for years to come. Healthcare, education, government and technology companies have proven to be valuable targets over the past year and will continue to be attractive to threat actors as we move into 2022. Each industry faces unique challenges, with an ever-changing array of assets to protect while simultaneously facing strict budgets and limited resources. Though the future remains uncertain, one thing is clear: data is extremely valuable for cybercriminals and is, therefore, an appealing target.

Conclusion

As we look ahead, defenders can take five lessons from the vulnerability and threat landscape in 2021:

Reconceptualize, but don't forget about, the perimeter. As organizations further adopt cloud infrastructure, bring in more third-party service providers and continue to support a remote workforce they must be conscious of how these changes influence their security posture. Security leaders should regularly audit the trust relationships undergirding critical operations and examine how dependencies can be mitigated to reduce security risk. Organizations should also ensure they are still properly managing more traditional perimeter security like VPNs, routers and firewalls.

Focus on misconfigurations and legacy vulnerabilities to disrupt attack paths. Threat groups of all kinds exploited AD misconfigurations and known vulnerabilities that organizations have failed to mitigate over months and even years. Ransomware groups and their affiliates are financially motivated and seek out low-hanging fruit, largely targeting legacy vulnerabilities, particularly ones in VPNs, and seeking out access to AD to have the greatest impact on organizations. Ransomware was the root cause for more than half of the 1,825 breaches analyzed; however, **6%** of breaches were the result of misconfigured, unsecured cloud databases. Defenders must continue to prioritize these known threats and not get distracted by flashy news stories. Ensuring proper system configuration may be the most valuable step organizations can take to reduce cyber risk.

Take a risk based approach to "everything as a service." The cloud shift, software as a service and infrastructure as a service all serve to give organizations a streamlined approach to conducting business, but at the trade-off of losing some control over security. While this means less maintenance and fewer patching concerns, the risk of misconfiguration or vulnerabilities introduced by the service provider should be a part of your threat model.

Worry about zero-days; worry more about legacy vulnerabilities. While zero-day vulnerabilities are cause for great concern, they are typically leveraged as part of targeted attacks. It is when a zero-day becomes a legacy vulnerability, and proof-of-concept exploit code is publicly available that they are abused more broadly by threat actors. Organizations need to ensure proper patching cadence and procedures in place for out-of-band patching. These models should also consider the criticality of assets in question and rollback plans and playbooks should a patch cause unexpected behavior.

Supply chain risks present unique challenges. Attackers have set their sights on supply chains of all types. In addition to the physical supply chain, threat actors have compromised software providers, hoping to sneak in malware that is later installed by unsuspecting victims. While this is an industry issue, organizations should ensure they take appropriate measures by maintaining backups, including off-site/off network backups and developing disaster recovery plans.

How Tenable can help

Tenable has released scan templates for Tenable.io, Tenable.sc and Nessus Professional which are pre-configured to allow quick scanning for the vulnerabilities discussed in this report. In addition, Tenable.io customers have a new dashboard and widgets in the widgets library and Tenable.sc users also have a new dashboard covering the 2021 Threat Landscape Retrospective.

SECTION 3

A Closer Look at the Key Vulnerabilities in 2021

The checklist below, organized by vendors, provides details on the year's most significant vulnerabilities with additional insights on how they're being exploited.

Zero-day | Noteworthy | Exploited in the Wild | Top 5

Accellion

FILE TRANSFER APPLIANCE (FTA)

CVE-2021-27101 is a SQL injection vulnerability. An unauthenticated, remote attacker could exploit the flaw by sending a specially crafted request as part of the Host header to the document_root file on a vulnerable FTA endpoint.

CVE-2021-27103 is a server-side request forgery (SSRF) vulnerability. An unauthenticated, remote attacker could exploit the flaw by sending a specially crafted HTTP POST request to the wmProgressstat file on a vulnerable FTA endpoint.

CVE-2021-27104 and CVE-2021-27102 are operating system (OS) command injection vulnerabilities. An unauthenticated, remote attacker could exploit CVE-2021-27104 by sending a specially crafted HTTP POST request to an FTA administrative endpoint. CVE-2021-27102 can be exploited via a local web service call by a local, low privilege attacker.

These four vulnerabilities were exploited in late 2020 and early in 2021 and are the root cause for data breaches at dozens of organizations.

Adobe

ADOBE READER

CVE-2021-21017 is a heap-based buffer overflow vulnerability in Adobe Reader. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires a victim to open a malicious file.

CVE-2021-28550 is a use-after-free vulnerability in Adobe Reader. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this vulnerability requires a victim to open a malicious file.

APACHE HTTP SERVER

CVE-2021-41773 is a path traversal and file disclosure vulnerability in Apache HTTP Server. A remote, unauthenticated attacker could exploit this vulnerability by sending a specially crafted request to a vulnerable web server. Successful exploitation would give an attacker access to arbitrary files outside of the document root on the web server. It could also leak sensitive information from interpreted CGI scripts.

CVE-2021-42013 is a path traversal and file disclosure vulnerability in Apache HTTP Server. It is a patch bypass for CVE-2021-41773, as the fix for it was insufficient. Even after applying the initial patch, a remote, unauthenticated attacker could exploit this vulnerability to map URLs to files outside of the document root.

APACHE LOG4J 2

CVE-2021-44228 is a remote code execution (RCE) vulnerability in Apache Log4j 2. An unauthenticated, remote attacker could exploit this flaw by sending a specially crafted request to a server running a vulnerable version of log4j. The crafted request uses a Java Naming and Directory Interface (JNDI) injection via a variety of services including:

- Lightweight Directory Access Protocol
- Secure LDAP
- Remote Method Invocation
- Domain Name Service

If the vulnerable server uses Log4j to log requests, the exploit will then request a malicious payload over JNDI through one of the services above from an attacker-controlled server. Successful exploitation could lead to RCE.

IOS: NO-CVE-ID - WIFIDEMON

Researchers at ZecOps disclosed a 0-click Wi-Fi format-string vulnerability in Apple iOS versions 14 through 14.4 that they named WiFiDemon. The flaw was silently patched in iOS 14.6 but never received a CVE identifier. ZecOps also reported exploitation of this flaw in the wild. An attacker could use this vulnerability to infect a target device without any user interaction if the Auto-Join Wi-Fi feature is enabled, which it is by default. The primary impact of this flaw is Dos but ZecOps asserts it could also lead to RCE.

M1 CHIPS

CVE-2021-30747 is a cover channel vulnerability in Apple's silicon M1 chip. It allows two applications running on the same OS to covertly exchange information. It is notable because it's the first vulnerability publicly disclosed in Apple M1 chips that requires a silicon redesign but, according to the researcher himself, "nobody's going to actually find a nefarious use for this flaw in practical circumstances."

MAC OS: CVE-2021-30892

CVE-2021-30892 is an inherited permissions flaw in Apple's macOS Big Sur and Monterey OSes that can be exploited to install rootkits. An attacker can use a specially crafted package with malicious post-install scripts to gain root access. This vulnerability was discovered by the Microsoft 365 Defender Research Team and named "Shrootless."

MAC OS, IOS, IPADOS, MACOS, WATCHOS: CVE-2021-1782

CVE-2021-1782 is a race condition in the iOS, iPadOS, macOS, watchOS and tvOS kernel. An attacker could craft a malicious application that could exploit this flaw and in order to elevate privileges.

IOS: CVE-2021-30895, CVE-2021-30896

CVE-2021-30895, CVE-2021-30896 are logic vulnerabilities in the Game Center for iOS and iPadOS. A specially crafted malicious application that exploits these vulnerabilities could read sensitive information, such as a user's contacts as well as their gameplay data.

IOS, IPADOS

NO-CVE-ID-ASSIGNED, NO-CVE-ID-ASSIGNED are two vulnerabilities in the com.apple.nehelper in iOS and iPadOS. They can be used by an attacker to enumerate installed applications on the device and gain access to WiFi information without the required entitlement. At the time this report was compiled, Apple had not yet fixed these flaws.

IOS, IPADOS, WATCHOS: CVE-2021-1879

CVE-2021-1879 is a use-after-free vulnerability in the QuickTimePluginReplacement in Safari. To exploit this flaw, an attacker would need to convince a target to visit a malicious website containing specially crafted content. Successful exploitation would lead to universal cross-site scripting. For more information about how this vulnerability was used, please visit this blog post from researchers at Google's Threat Analysis Group.

MAC OS, IOS, IPADOS, TVOS, WATCHOS: CVE-2021-30883

CVE-2021-30883 is a memory corruption vulnerability in the iOMobileFrameBuffer of iOS, iPadOS, macOS, tvOS and watchOS. An attacker could craft a malicious application that could exploit this flaw. If a target were to open the malicious application, it would execute arbitrary code with kernel privileges.

IOS, IPADOS, MACOS, TVOS, WATCHOS: CVE-2021-30860

CVE-2021-30860 is an integer overflow vulnerability in the CoreGraphics library on iOS, iPadOS, watchOS and macOS. To exploit this flaw, an attacker would need to create a specially crafted PDF file containing the exploit code. Successful exploitation would result in arbitrary code execution. User interaction is not required to exploit this flaw and researchers have called it a zero-click vulnerability. For more details, please read CitizenLab's blog post.

IOS, IPADOS, MACOS, WATCHOS, TVOS: CVE-2021-30665

CVE-2021-30665 is a memory corruption vulnerability in iOS, iPadOS, macOS, watchOS and tvOS. To exploit this flaw, an attacker would need to convince a target to visit a malicious website containing specially crafted content. Successful exploitation would result in arbitrary code execution.

IOS, IPADOS, WATCHOS, MACOS: CVE-2021-30807

CVE-2021-30807 is a memory corruption vulnerability in the iOMobileFrameBuffer in iOS, iPadOS, watchOS and macOS. An attacker could craft a malicious application that could exploit this flaw. If a target were to open the malicious application, it would execute arbitrary code with kernel privileges.

MAC OS: CVE-2021-30657

CVE-2021-30657 is a logic vulnerability in the macOS policy subsystem, syspolicyd. A specially crafted malicious application could bypass the macOS Gatekeeper. For more details about this vulnerability, please read the following blog posts from Cedric Owens and Patrick Wardle.

MAC OS: CVE-2021-30713

CVE-2021-30713 is a validation issue in the Transparency, Consent and Control (TCC) system in macOS. A specially crafted malicious application could be used to bypass Privacy preferences.

MACOS: NO-CVE-ID-ASSIGNED

NO-CVE-ID-ASSIGNED is a RCE vulnerability in Finder for macOS. To exploit the vulnerability, an attacker would need to embed a file containing a specially crafted command and convince a target to open this file, for instance, as part of an email attachment. This vulnerability was silently patched and no CVE-ID was assigned. However, the patch was insufficient and Apple has not released an updated patch at the time this report was compiled.

MAC OS: CVE-2021-30869

CVE-2021-30869 is a type confusion vulnerability in the XNU kernel of macOS. A specially crafted malicious application could execute arbitrary code with kernel privileges. For more information about this vulnerability, please read Google's Threat Analysis Group blog post.

MACOS, IOS, IPADOS: CVE-2021-1870 AND CVE-2021-1871

CVE-2021-1870 and CVE-2021-1871 are logic issues in WebKitGTK and WPE WebKit. A remote attacker could exploit these vulnerabilities to gain arbitrary code execution.

IOS: CVE-2021-30761

CVE-2021-30761 is a memory corruption vulnerability in WebKitGTK. To exploit this flaw, an attacker would need to convince a target to visit a malicious website containing specially crafted content. Successful exploitation would result in arbitrary code execution.

IOS: CVE-2021-30762

CVE-2021-30762 is a use-after-free vulnerability in WebKitGTK. To exploit this flaw, an attacker would need to convince a target to visit a malicious website containing specially crafted content. Successful exploitation would result in arbitrary code execution.

IOS, IPADOS, MACOS, WATCHOS, TVOS: CVE-2021-30661

CVE-2021-30661 is a use-after-free vulnerability in WebKit Storage for iOS, iPadOS, macOS, watchOS and tvOS. To exploit this flaw, an attacker would need to convince a target to visit a malicious website containing specially crafted content. Successful exploitation would result in arbitrary code execution.

IOS: CVE-2021-30666

CVE-2021-30666 is a buffer overflow vulnerability in WebKit. To exploit this flaw, an attacker would need to convince a target to visit a malicious website containing specially crafted content. Successful exploitation would result in arbitrary code execution.

IOS, IPADOS, TVOS, MACOS: CVE-2021-30663

CVE-2021-30663 is an integer overflow vulnerability in WebKit for iOS, iPadOS, tvOS and macOS. To exploit this flaw, an attacker would need to convince a target to visit a malicious website containing specially crafted content. Successful exploitation would result in arbitrary code execution.

IOS, IPADOS, MACOS: CVE-2021-30858

CVE-2021-30858 is a use-after-free vulnerability in WebKit for iOS, iPadOS and macOS. To exploit this flaw, an attacker would need to convince a target to visit a malicious website containing specially crafted content. Successful exploitation would result in arbitrary code execution.

arm

CVE-2021-28663

CVE-2021-28663 is a use-after-free vulnerability in the Arm Mali graphics processing units (GPU) kernel driver that could be exploited for privilege escalation or information disclosure.

CVE-2021-28664

CVE-2021-28664 is an improper privilege management vulnerability in the Arm Mali GPU kernel driver that could be exploited for privilege escalation or a denial of service (memory corruption).

CVE-2021-42258

CVE-2021-42258 is a SQL injection vulnerability in BQE's BillQuick Web Suite software. A remote, unauthenticated attacker could exploit this vulnerability by sending a specially crafted request to the vulnerable BillQuick Web Suite server. Successful exploitation would grant an attacker arbitrary code execution.

CVE-2021-42344, CVE-2021-42345, CVE-2021-42346, CVE-2021-42571, CVE-2021-42572, CVE-2021-42573, CVE-2021-42741, CVE-2021-42742

CVE-2021-42344, CVE-2021-42345, CVE-2021-42346, CVE-2021-42571, CVE-2021-42572, CVE-2021-42573, CVE-2021-42741, CVE-2021-42742 are several vulnerabilities in the BillQuick Web Suite software discovered by researchers at Huntress Labs. At the time this report was compiled, there were no patches available to address these flaws. As a result, there are no vulnerability details about these CVEs.

SMALL BUSINESS VPN ROUTERS: CVE-2021-1609

CVE-2021-1609 is a RCE and denial of service (DoS) vulnerability in Cisco's web management interface for Cisco Small Business routers that was assigned a CVSSv3 score of 9.8. A remote, unauthenticated attacker could exploit the vulnerability by sending a specially crafted HTTP request to a vulnerable device, resulting in arbitrary code execution as well as the ability to reload the device, resulting in a denial of service.

SMALL BUSINESS VPN ROUTERS: CVE-2021-1610

CVE-2021-1610 is a command injection vulnerability in the same web management interface. While both flaws exist due to improper validation of HTTP requests and can be exploited by sending specially crafted HTTP requests, CVE-2021-1610 can only be exploited by an authenticated attacker with root privileges. Successful exploitation would grant an attacker the ability to gain arbitrary command execution on the vulnerable device's operating system.

These vulnerabilities can be exploited independently of each other, and some versions of the Small Business VPN Router software may only be affected by one of the two vulnerabilities.

Confluence

CONFLUENCE SERVER AND CONFLUENCE DATA CENTER: CVE-2021-26084

CVE-2021-26084 is an Object-Graph Navigation Language injection vulnerability in the Atlassian Confluence Webwork implementation. An unauthenticated, remote attacker could exploit this flaw by sending a specially crafted request to vulnerable endpoints on the Confluence Server or Data Center instance. Successful exploitation would allow an attacker to execute arbitrary code. This vulnerability was exploited in the wild to install cryptominers shortly after it was patched in August.

BIG-IP AND BIG-IQ

In March, F5 published advisories and patches for several critical flaws in BIG-IP and BIG-IQ, a family of hardware and software solutions for application delivery and centralized device management. The most concerning vulnerability is CVE-2021-22986 because it doesn't require authentication and successful exploitation would "lead to complete system compromise."

CVE-2021-22992 is a buffer-overflow vulnerability in the Advanced Web Application Firewall or Application Security Manager virtual server due to the way the Login Page is configured. At a minimum, an attacker would be able to cause a DoS and, in some instances, gain arbitrary code execution privileges. A list of the vulnerabilities identified is included in the table below:

CVE	Desecription	CVSSv3
CVE-2021-22986	Unauthenticated Remote Code Execution	9.8
CVE-2021-22987	Authenticated Remote Code Execution	9.9
CVE-2021-22988	Authenticated Remote Code Execution	8.8
CVE-2021-22989	Authenticated Remote Code Execution	9.1
CVE-2021-22990	Authenticated Remote Code Execution	7.2
CVE-2021-22991	Buffer Overflow and Denial of Service	9.8
CVE-2021-22992	Buffer Overflow and Denial of Service	9.8

ENTROLINK

NO-CVE-ID-ASSIGNED is a code injection vulnerability in PPX-AnyLink devices. A remote, unauthenticated attacker could exploit this vulnerability by sending a specially crafted request to a vulnerable device. At the time this report was compiled, there was no patch available for this vulnerability.

CVE-2021-27860

CVE-2021-27860 (also identified as FPSA006) is a vulnerability in the web management interface of several FatPipe devices including its MPVPN, IPVPN, and WARP. A remote, unauthenticated attacker could exploit this vulnerability by sending a specially crafted HTTP request to a vulnerable device. Successful exploitation would grant an attacker root access to the device.

FORTINET: CVE-2018-13379

CVE-2018-13379 is a path traversal vulnerability in Fortinet's FortiGate SSL VPN. An unauthenticated, remote attacker could exploit this vulnerability by sending a specially crafted request containing a path traversal sequence to a vulnerable Fortigate SSL VPN endpoint. This would allow the attacker to read arbitrary files from the device including the contents of the "sslvpn_websesion" session file that contains both usernames and plaintext passwords.

FORTINET: CVE-2019-5591

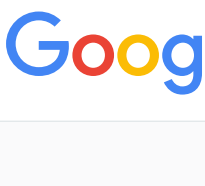
CVE-2019-5591 is a default configuration vulnerability in the FortiGate SSL VPN. Under the default configuration, when a Lightweight Directory Access Protocol (LDAP) server sends a connection request to the FortiGate device, the certificate is not verified. To exploit the vulnerability, an attacker could connect to a vulnerable FortiGate device by impersonating an LDAP server. Successful exploitation would allow the attacker to harvest sensitive information intended for a legitimate LDAP server.

FORTINET: CVE-2020-12812

CVE-2020-12812 is an improper authentication vulnerability in the FortiGate SSL VPN. This vulnerability exists due to settings used for two-factor authentication — specifically, when two-factor authentication has been enabled under the "user local" setting, but the authentication type is set to remote authentication, such as LDAP. If a VPN user changes the case of their username, a mismatch occurs, and the device won't prompt for a second factor, allowing an attacker to bypass the two-factor authentication requirement.

GHOSTSCRIPT: CVE-2021-3781

CVE-2021-3781 is a sandbox escape vulnerability in the Ghostscript interpreter. An attacker could exploit the vulnerability by creating a specially crafted file that is interpreted by Ghostscript. Successful exploitation would grant an attacker remote code execution.



CVE-2021-21166

CVE-2021-21166 is a data race vulnerability in the Web Audio application programming interface (API) for Google Chrome and other chromium-based browsers. A remote attacker could exploit this vulnerability by convincing a target to visit a specially crafted HTML page using a vulnerable browser.

CVE-2021-21193 AND CVE-2021-21206

CVE-2021-21193 and CVE-2021-21206 are use-after-free vulnerabilities in the Blink rendering engine for Google Chrome and other chromium-based browsers. A remote attacker could exploit these vulnerabilities by convincing a target to visit a specially crafted HTML page using a vulnerable browser.

V8 ENGINE

The following are several vulnerabilities in V8, an open-source engine used by Chromium-based projects including Google Chrome. A remote attacker could exploit these vulnerabilities by convincing a target to visit a specially crafted HTML page using a vulnerable browser.

CVE	Vulnerability Type
CVE-2021-21148	Heap Buffer Overflow
CVE-2021-21220	Insufficient Validation of Untrusted Input
CVE-2021-21224*	Type Confusion
CVE-2021-30551	Type Confusion
CVE-2021-30563	Type Confusion
CVE-2021-37975	Use-After-Free
CVE-2021-30632	Out-of-Bounds Write
CVE-2021-38003	Inappropriate Implementation
CVE-2021-4102	Use-After-Free

*Successful exploitation would give an attacker arbitrary code execution privileges in the browser sandbox

CVE-2021-30554

CVE-2021-30554 is a use-after-free vulnerability in webGL for Google Chrome and other chromium-based browsers. A remote attacker could exploit this vulnerability by convincing a target to visit a specially crafted HTML page using a vulnerable browser.

CVE-2021-30633

CVE-2021-30633 is a use-after-free vulnerability in the Indexed DB API in Google Chrome and other chromium-based browsers. A remote attacker could exploit this vulnerability by convincing a target to visit a specially crafted HTML page using a vulnerable browser. Successful exploitation could grant an attacker the ability to escape the browser sandbox if the renderer process had been compromised.

CVE-2021-37973

CVE-2021-37973 is a use-after-free vulnerability in the Portals API in Google Chrome and other chromium-based browsers. A remote attacker could exploit this vulnerability by convincing a target to visit a specially crafted HTML page using a vulnerable browser. Successful exploitation could grant an attacker the ability to escape the browser sandbox if the renderer process had been compromised.

CVE-2021-37976

CVE-2021-37976 is an inappropriate implementation in Memory in Google Chrome and other chromium-based browsers. A remote attacker could exploit this vulnerability by convincing a target to visit a specially crafted HTML page using a vulnerable browser. Successful exploitation could grant an attacker the ability to obtain sensitive information from the process memory of the browser.

CVE-2021-38000

CVE-2021-38000 is an insufficient validation of trusted input in Intents in Google Chrome on Android. A remote attacker could arbitrarily force the vulnerable browser to visit a malicious URL by convincing the victim to visit a specially crafted HTML page.

CVE-2021-1048

CVE-2021-1048 is an elevation of privilege vulnerability in the Android upstream kernel.

CVE-2021-22893

CVE-2021-22893 is an authentication bypass vulnerability in Pulse Connect Secure. A remote, unauthenticated attacker could exploit this vulnerability by sending a specially crafted HTTP request to a vulnerable device. Successful exploitation of this vulnerability would grant an attacker the ability to execute arbitrary code on the Pulse Connect Secure Gateway.

CVE-2021-22937

CVE-2021-22937 is an uncontrolled archive extraction vulnerability in the Pulse Connect Secure appliance that allows an authenticated administrator to write arbitrary executable files to the "/home/runtime/tmp/tt/" directory. Successful exploitation would give attackers root privileges on the targeted appliance. It is a patch bypass for CVE-2020-8260, an unrestricted file upload vulnerability that was addressed in October 2020 and has been exploited by attackers.

CVE-2021-30116

CVE-2021-30116 is an insufficiently protected credentials vulnerability in the Kaseya Virtual System Administrator (VSA).

CVE-2021-30119

CVE-2021-30119 is a cross-site scripting vulnerability in the Kaseya VSA.

CVE-2021-30120

CVE-2021-30120 is an incorrect authorization vulnerability in Kaseya VSA that can bypass two-factor authentication.

All three vulnerabilities (CVE-2021-30116, CVE-2021-30119, CVE-2021-30120) were used as part of an attack by the REvil ransomware group in July, targeting customers of managed service providers that used VSA for remote monitoring and management.

CVE-2021-40385

CVE-2021-40385 is an elevation of privilege vulnerability in Kaseya Unitrends Backup Software. Successful exploitation of this vulnerability would grant an attacker the ability to elevate privileges from read-only to administrator.

CVE-2021-40387

CVE-2021-40387 is an authenticated remote code execution vulnerability in Kaseya Unitrends Backup Software.

CVE-2021-40386

CVE-2021-40386 is an undisclosed, critical vulnerability in the Kaseya Unitrends Backup Client/Agent. Kaseya was informed about the vulnerability by researchers, but at the time this report was compiled, no details about this vulnerability were public.

Microsoft

AZURE: CHAOSDB (NO-CVE-ID)

ChaosDB is a critical vulnerability in Azure Cosmos DB, Microsoft's fully managed NoSQL database. To exploit the flaw, an attacker would need to chain vulnerabilities in the Jupyter Notebook feature of Azure Cosmos DB to query data like credentials to Cosmos DB accounts, Jupyter Notebook Compute and Jupyter Notebook Storage. These credentials would allow an attacker to gain full administrator access to Cosmos DB. Microsoft has patched the issue, however researchers at Wiz, who discovered the flaw, note that the issue may have existed for months prior to its discovery.

AZURE: AZURESCAPE (NO-CVE-ID)

According to researchers at Palo Alto's Unit 42, Azurescape is the first known cloud cross-account container takeover vulnerability that would allow a malicious user to execute code on other users' containers and take full control over them. Exploitation is a three step process that would allow a malicious Azure user to compromise multitenant Kubernetes clusters that host Azure Container Instances (ACI). The attack works by first deploying a container image which exploits CVE-2019-5736, a two year old container breakout issue in runC, a widely used container runtime in container images including ACI. The image will break out of the ACI container when executed. After this, the attacker can gain administrative privileges and execute malicious code on a multitenant Kubernetes cluster.

AZURE: CVE-2021-38646 "OMIGOD"

CVE-2021-38645, CVE-2021-38647, CVE-2021-38648, CVE-2021-38649, also known as OMIGOD, are four vulnerabilities in Microsoft's Open Management Infrastructure (OMI) open source project in Azure Cloud. OMI is used for managing configurations across local and remote environments and the OMI agent is automatically deployed on Azure virtual machines that have certain services enabled. These services include:

- Azure Automation
- Azure Automatic Update
- Azure Operations Management Suite
- Azure Log Analytics
- Azure Configuration Management
- Azure Diagnostics
- Azure Container Insights

Please note that this may not be a complete list and additional services may deploy OMI.

The most severe vulnerability of the four is CVE-2021-38647, an unauthenticated RCE vulnerability with a 9.8 CVSSv3 score. Because OMI runs as root, a low privileged user or external attacker could use a Unix socket or communicate over an HTTP API to execute code on a victim machine with a single request. This vulnerability was exploited in the wild and has at least 12 public PoCs on GitHub at the time this report was compiled. The remaining CVEs, CVE-2021-38645, CVE-2021-38648 and CVE-2021-38649 are elevation of privilege vulnerabilities in OMI. According to the vulnerability disclosure, CVE-2021-38648 is "remarkably similar" to CVE-2021-38647 in that the exploitation process is nearly the same, however the root cause is different.

EXCEL: CVE-2021-42292

CVE-2021-42292 is a security feature bypass in Microsoft Excel. To exploit this vulnerability, an attacker would need to convince their target to open a malicious Excel document.

EXCHANGE SERVER: CVE-2021-26855

CVE-2021-26855 is a SSRF vulnerability dubbed ProxyLogon by Orange Tsai, the researcher credited with its discovery. An unauthenticated, remote attacker could exploit this flaw by sending a specially crafted HTTP request to a vulnerable Exchange Server that accepts untrusted connections over port 443. Successful exploitation of this flaw would allow the attacker to authenticate to the targeted Exchange Server.

EXCHANGE SERVER: CVE-2021-26857

CVE-2021-26857 is an insecure deserialization vulnerability. Specifically, the flaw resides in the Exchange Unified Messaging Service, which enables voice mail functionality in addition to other features. To exploit this flaw, an attacker would need to be authenticated to the vulnerable Exchange Server with administrator privileges, potentially by exploiting another vulnerability first. Successful exploitation would grant the attacker arbitrary code execution privileges as SYSTEM.

EXCHANGE SERVER: CVE-2021-26858 AND CVE-2021-27065

CVE-2021-26858 and CVE-2021-27065 are arbitrary file write vulnerabilities. These flaws are post-authentication, meaning an attacker would first need to authenticate to the vulnerable Exchange Server before they could exploit them. This could be achieved by exploiting CVE-2021-26855 or by using stolen administrator credentials. Once authenticated, an attacker could arbitrarily write to any paths on the vulnerable server.

EXCHANGE SERVER: PROXYSHELL

ProxyShell is a chain of three CVEs: CVE-2021-34473, a RCE vulnerability; CVE-2021-34523, an elevation of privilege (EoP) and CVE-2021-31207, a feature bypass. By chaining these vulnerabilities, an attacker could execute arbitrary commands on vulnerable Exchange servers on port 443. Two of the three ProxyShell vulnerabilities, CVE-2021-34473 and CVE-2021-34523, were patched as part of the April 2021 Patch Tuesday release, though Microsoft says they were "inadvertently omitted" from that security update guide. CVE-2021-31207 was patched in May.

EXCHANGE SERVER: CVE-2021-42321

CVE-2021-42321 is a RCE that exists due to the improper validation of command-let (cmdlet) arguments. To exploit this vulnerability, an attacker would need to be authenticated to a vulnerable Exchange Server. Microsoft says they are aware of "limited targeted attacks" using this vulnerability in the wild. Additionally, this appears to be the same vulnerability in Exchange Server that was exploited at the Tianfu Cup, a Chinese cybersecurity contest.

INTERNET EXPLORER: CVE-2021-26411

CVE-2021-26411 is a memory corruption vulnerability in Internet Explorer that was exploited in the wild as a zero-day. In order to exploit the flaw, an attacker would need to host the exploit code on a malicious website and convince a user through social engineering tactics to visit the page, or the attacker could inject the malicious payload into a legitimate website.

INTERNET EXPLORER: CVE-2021-27085

CVE-2021-27085 is a RCE vulnerability in Internet Explorer. A remote, unauthenticated attacker could exploit this vulnerability by convincing a target to visit a malicious website containing exploit code or injecting exploit code into a legitimate website.

NETLOGON: ZEROLOGON (CVE-2021-1472)

CVE-2020-1472, known as Zerologon, is an EoP vulnerability in Microsoft's Netlogon Remote Protocol (MS-NRPC). This protocol is used to maintain relationships of domain controllers (DCs) within and across domains. Critically, MS-NRPC is also used to manage account changes for DCs, like passwords. The flaw exists because of a flaw in how MS-NRPC implements AES-CFB8 encryption. Because this is a local privilege escalation flaw, an attacker needs to be on the same local area network as their target. Active Directory (AD) is a target of serious concern with Zerologon. If an attacker was able to exploit it against AD, they could impersonate any machine on the network, reset the domain controller's administrator password or launch ransomware attacks against the entire network.

NTLM: CVE-2021-36942

CVE-2021-36942 is a Windows LSA Spoofing Vulnerability that was patched in August in relation to the PetitPotam NTLM relay attack disclosed by Gilles Lionel. The exploit could be used to force domain controllers to authenticate with an attacker-controlled destination. Roughly a month after disclosure, ransomware groups were seen exploiting this attack. The patch for CVE-2021-36942 only partially patched the issue. Microsoft published general mitigation guidance for defending against NTLM Relay Attacks. The LockFile ransomware has chained Microsoft Exchange vulnerabilities with PetitPotam to take over domain controllers.

PRINT SPOOLER: PRINTNIGHTMARE (CVE-2021-1675 AND CVE-2021-34527)

CVE-2021-1675 and CVE-2021-34527 are RCE vulnerabilities in the Windows Print Spooler Service, which is available across desktop and server versions of Windows operating systems. The service is used to manage printers and print servers. The vulnerabilities exist because the service does not handle privileged file operations properly. An authenticated, remote or local attacker could exploit these flaws to gain arbitrary code execution with SYSTEM privileges. Both flaws are interchangeably referred to as PrintNightmare.

PRINT SPOOLER: CVE-2021-34481

CVE-2021-34481 is a RCE that was originally labeled as an EoP. It was disclosed as a zero-day in an out-of-band informational advisory on July 15. Jacob Baines, credited with discovering CVE-2021-34481, presented his work at DEF CON 29 and published an exploit tool on GitHub. This vulnerability allows a low privilege user to install vulnerable print drivers to a target system which can then be exploited to achieve SYSTEM privileges.

PRINT SPOOLER: CVE-2021-36936 AND CVE-2021-36947

CVE-2021-36936 and CVE-2021-36947 are RCE vulnerabilities in Windows Print Spooler that were patched as part of the August Patch Tuesday release.

PRINT SPOOLER: CVE-2021-34483

CVE-2021-34483 is an EoP vulnerability, also patched in August. It was credited to Victor Mata with FusionX at Accenture Security and Thibault van Geluwe. Mata states that he originally reported CVE-2021-34483 to Microsoft in December and did not publish details per Microsoft's request.

PRINT SPOOLER: CVE-2021-36958

CVE-2021-36958 is another vulnerability disclosed as a zero-day in an out-of-band informational advisory on August 11. CVE-2021-36958 is also credited to Mata and was publicly disclosed by Benjamin Delpy on Twitter in July.

PRINT SPOOLER: CVE-2021-36970

CVE-2021-36970 is a spoofing vulnerability in the Windows Print Spooler that received a CVSSv3 score of 8.8 and the designation of "Exploitation More Likely" according to Microsoft's Exploitability Index. This vulnerability requires that an attacker have access to the same network as a target and user interaction.

PRINT SPOOLER: CVE-2021-38667, CVE-2021-38671 AND CVE-2021-40447

CVE-2021-38667, CVE-2021-38671 and CVE-2021-40447 are EoP vulnerabilities in Windows Print Spooler. All three vulnerabilities were assigned a CVSSv3 score of 7.8 and are rated Important. Of the three vulnerabilities, CVE-2021-38671 is the only flaw rated as Exploitation More Likely.

MSHTML (TRIDENT): CVE-2021-33742

CVE-2021-33742 is a RCE vulnerability in the Windows MSHTML (Trident) platform, Microsoft's proprietary browser engine. A remote, unauthenticated attacker could exploit this vulnerability by convincing a target to open a specially crafted file or visit a malicious website using an affected application.

MSHTML (TRIDENT): CVE-2021-40444

CVE-2021-40444 is a RCE vulnerability in Microsoft's MSHTML (Trident) platform, Microsoft's proprietary browser engine. To exploit this vulnerability, an attacker would need to create a specially crafted Microsoft Office document containing a malicious ActiveX control and use social engineering techniques to convince their target to open the document. The impact of this vulnerability would be more significant in cases where the recipient has administrative privileges.

WIN32K: CVE-2021-1732

CVE-2021-1732 is an EoP vulnerability due to the Windows kernel-mode driver improperly handling objects in memory. To exploit this vulnerability, an attacker must first gain a foothold in a vulnerable system. Successful exploitation would elevate the privileges of an attacker, potentially allowing them to create new accounts, install programs and view, modify or delete data.

WIN32K: CVE-2021-40449

CVE-2021-40449 is a use-after-free elevation of privilege vulnerability in Win32k. A local, authenticated attacker could exploit this vulnerability to gain elevated privileges. It is a patch-bypass for CVE-2016-3309, another elevation of privilege vulnerability.

CVE-2021-31199 AND CVE-2021-31201

CVE-2021-31199 and CVE-2021-31201 are EoP vulnerabilities in Microsoft's Enhanced Cryptographic Provider. A local, authenticated attacker could exploit this vulnerability to gain elevated privileges. It is related to CVE-2021-28550, a use-after-free vulnerability in Adobe Reader.

CVE-2021-33739

CVE-2021-33739 is an EoP vulnerability in the Microsoft Desktop Window Manager core library, dwmcore.dll. To exploit this vulnerability, an attacker must first gain a foothold in a vulnerable system. Successful exploitation would elevate the privileges of an attacker, potentially allowing them to create new accounts, install programs, and view, modify or delete data.

CVE-2021-31955

CVE-2021-31955 is an information disclosure vulnerability in the Windows Kernel (ntoskrnl.exe). An attacker could use this vulnerability to disclose information from the system, such as kernel addresses. They could then combine this with CVE-2021-31956 to elevate privileges on the targeted system.

CVE-2021-31956

CVE-2021-31956 is an EoP vulnerability in the Windows New Technology File System that could allow a local user to elevate their privileges on a vulnerable system. A local user could exploit the flaw with a crafted application in order to take control of a system.

CVE-2021-36934

CVE-2021-36934 is an EoP vulnerability in Microsoft Windows. An authenticated, local attacker could exploit this vulnerability to run arbitrary code with SYSTEM privileges, potentially allowing them to create new accounts, install programs, and view, modify or delete data. To exploit this vulnerability, an attacker needs to have sufficient privileges to execute code on a victim's system.

OPEN SOURCE

DISCOURSE: CVE-2021-41163

CVE-2021-41163 is a RCE in the open source discussion forum and mailing list management platform Discourse. It received the maximum CVSSv3 score 10.0 and CISA issued an advisory urging developers to apply the emergency patch or workarounds.

DNSMASQ

JSOF research labs disclosed seven vulnerabilities they discovered in the open source DNS forwarding software. Named DNSpooq, the seven flaws can be divided into two categories: DNS cache poisoning and buffer overflow. The buffer overflow vulnerabilities can be used to gain RCE, however they are more likely to result in DoS when successfully exploited.

CVE	Impact	CVSSv3
CVE-2020-25684	DNS Cache Poisoning	4
CVE-2020-25685	DNS Cache Poisoning	4
CVE-2020-25686	DNS Cache Poisoning	4
CVE-2020-25681	Remote Code Execution, Denial of Service	8.1
CVE-2020-25682	Remote Code Execution, Denial of Service	8.1
CVE-2020-25683	Remote Code Execution, Denial of Service	5.9
CVE-2020-25687	Remote Code Execution, Denial of Service	5.9

EXIM: 21NAILS

The Qualys Research Team reviewed the code for Exim and **uncovered 21 vulnerabilities** it named 21Nails. Of those 21, ten of these vulnerabilities can be exploited remotely and the remaining eleven can only be exploited locally. The advisory notes that most of them can be exploited in either the default configuration or in common configurations. They further state that chaining of a few of these vulnerabilities could allow an attacker remote unauthenticated code execution and the ability to gain root privileges on the Exim Server. According to the blog post, all versions of Exim prior to 4.94.1 are affected by the following CVEs:

CVE	Impact	CVSSv3
CVE-2020-28007	Link attack in Exim's log directory	7.8
CVE-2020-28008	Assorted attacks in Exim's spool directory	7.8
CVE-2020-28009	Integer overflow in get_stdinput()	7.8
CVE-2020-28010	Heap out-of-bounds write in main()	7.8
CVE-2020-28011	Heap buffer overflow in queue_run()	7.8
CVE-2020-28012	Missing close-on-exec flag for privileged pipe	7.8
CVE-2020-28013	Heap buffer overflow in parse_fix_phrase()	7.8
CVE-2020-28014	Arbitrary file creation and clobbering	6.1
CVE-2020-28015	New-line injection into spool header file (local)	7.8
CVE-2020-28016	Heap out-of-bounds write in parse_fix_phrase()	7.8
CVE-2020-28017	Integer overflow in receive_add_recipient()	9.8
CVE-2020-28018	Use-after-free in tls-openssl.c	9.8
CVE-2020-28019	Failure to reset function pointer after BDAT error	7.5
CVE-2020-28020	Integer overflow in receive_msg()	9.8
CVE-2020-28021	New-line injection into spool header file (remote)	8.8
CVE-2020-28022	Heap out-of-bounds read and write in extract_option()	9.8
CVE-2020-28023	Out-of-bounds read in smtp_setup_msg()	7.5
CVE-2020-28024	Heap buffer underflow in smtp_ungetc()	9.8
CVE-2020-28025	Heap out-of-bounds read in pdkim_finish_bodyhash()	7.5
CVE-2020-28026	Line truncation and injection in spool_read_header()	9.8
CVE-2021-27216	Arbitrary file deletion	6.3

EXIM: GOCD: CVE-2021-43286, CVE-2021-43287, CVE-2021-43288 AND CVE-2021-43289

CVE-2021-43286, CVE-2021-43287, CVE-2021-43288 and CVE-2021-43289 are all flaws in GoCD, an open source continuous delivery tool, that could facilitate supply chain attacks. Exploitation of these vulnerabilities could give attackers access to intellectual property and production environments, allowing them to modify code.

GRUB2

CVE-2020-14372, CVE-2020-25632, CVE-2020-25647, CVE-2020-27749, CVE-2020-27779, CVE-2021-20225, CVE-2021-20233 and CVE-2021-3418 are a set of vulnerabilities discovered by several different researchers who began examining GRand Unified Bootloader version 2 (GRUB2) following the disclosure of the BootHole flaw in 2020. GRUB2 is Windows and Linux software that loads an OS into memory when a system boots up. Several of these vulnerabilities would allow an attacker to bypass Secure Boot.

LINUX KERNEL: CVE-2021-33909

CVE-2021-33909 is an out-of-bounds write vulnerability that could lead to EoP that impacts the majority of Linux distributions in their default configuration. It was discovered and named Sequoia by the Qualys Research Team. An unprivileged attacker could exploit this vulnerability to gain root privileges.

OPENSSL: CVE-2021-3449

CVE-2021-3449 is a DoS vulnerability caused by a null pointer dereference flaw in OpenSSL versions 1.1.1h to 1.1.1k. An attacker could crash vulnerable OpenSSL servers by sending a malicious renegotiation request from an unauthenticated end user during the secure handshake. A server is only vulnerable if it has TLSv1.2; OpenSSL TLS clients are not impacted by this issue.

SUDO: CVE-2021-3156

CVE-2021-3156 is a heap-based buffer overflow vulnerability named Baron Samedit. This vulnerability occurs when an allocated buffer in memory that is being overwritten exceeds the allocated space. This overflow happens in the heap portion of memory, which is where global variables are stored by default. A local, non-privileged user can pass a specially crafted command-line argument to sudo on a vulnerable system to exploit the flaw. CVE-2021-3156 could impact nearly all versions of Linux/Unix that include vulnerable versions of sudo (1.9.0 through 1.9.5p1 for stable versions and 1.82 through 1.8.31p2 for legacy).

WEBSVN: CVE-2021-32305

CVE-2021-32305 is an arbitrary code execution vulnerability caused by improper input sanitization. Shortly after the flaw was disclosed, Palo Alto Network's Unit 42 detected exploitation in the wild to launch distributed DoS attacks.

PROTOCOLS, STACKS AND SOFTWARE DEVELOPMENT KITS

BADALLOC

BadAlloc is a set of 27 critical memory allocation vulnerabilities found in libraries and real-time operating system (RTOS) used in a wide range of OT and IoT devices. All of the vulnerabilities could allow for RCE and are the result of the use of vulnerable memory functions that lack proper input validations. Microsoft worked in coordination with CISA and US-CERT to disclose these vulnerabilities. CISA maintains a list of the affected systems including responses from the vendors they were able to contact. We recommend reviewing the vendor responses for mitigation steps or patch options. The following table contains a list of the CVEs that make up BadAlloc.

CVE	Description	Affected RTOS	CVSSv3
CVE-2020-13603	Integer Overflow or Wraparound	Zephyr Project RTOS	7.8
CVE-2020-28895	Integer Overflow or Wraparound	Wind River VxWorks	7.3
CVE-2020-35198	Integer Overflow or Wraparound	Wind River VxWorks	9.8
CVE-2021-22156	Integer Overflow or Wraparound	BlackBerry QNX SDP	9.8
CVE-2021-22636	Integer Overflow or Wraparound	Texas Instruments TI-RTOS	7.4
CVE-2021-22680	Integer Overflow or Wraparound	NXP MQX	7.3
CVE-2021-22684	Integer Overflow or Wraparound	Samsung Tizen RT RTOS	7.5
CVE-2021-26461	Integer Overflow or Wraparound	Apache Nuttx OS	9.8
CVE-2021-26706	Integer Overflow or Wraparound	Micrium uC/OS: uC/LIB	6.5
CVE-2021-27411	Integer Overflow or Wraparound	Micrium OS	6.5
CVE-2021-27417	Integer Overflow or Wraparound	eCosCentric eCosPro RTOS	4.6
CVE-2021-27419	Integer Overflow or Wraparound	uClibc-ng	7.3
CVE-2021-27421	Integer Overflow or Wraparound	NXP MCUXpresso SDK	7.3
CVE-2021-27425	Integer Overflow or Wraparound	Cesanta Software Mongoose-OS	7.3
CVE-2021-27427	Integer Overflow or Wraparound	RIOT OS	7.3
CVE-2021-27429	Integer Overflow or Wraparound	Texas Instruments TI-RTOS	7.4
CVE-2021-27431	Integer Overflow or Wraparound	ARM CMSIS RTOS2	7.3
CVE-2021-27433	Integer Overflow or Wraparound	ARM mbed-ualloc	7.3
CVE-2021-27435	Integer Overflow or Wraparound	ARM mbed	7.3
CVE-2021-27439	Integer Overflow or Wraparound	TencentOS-tiny	7.3
CVE-2021-27502	Integer Overflow or Wraparound	Texas Instruments TI-RTOS	7.4
CVE-2021-27504	Integer Overflow or Wraparound	Texas Instruments devices running FREERTOS	7.4
CVE-2021-30636	Integer Overflow or Wraparound	Media Tek LinkIt SDK	7.3
CVE-2021-31571	Integer Overflow or Wraparound	Amazon FreeRTOS	9.8
CVE-2021-31572	Integer Overflow or Wraparound	Amazon FreeRTOS	9.8
CVE-2021-3420	Integer Overflow or Wraparound	Redhat newlib	9.8
Not Assigned	Integer Overflow or Wraparound	Google Cloud IoT Device SDK	N/A

DOMAIN NAME SERVER ECOSYSTEM

The tsuNAME vulnerability was discovered by a team of researchers from SIDN Labs, InternetNZ, the Information Science Institute and the University of Southern California. The vulnerability could be used to amplify traffic to perform DDoS attacks against authoritative DNS servers. This vulnerability exists because of how some DNS resolver software handles misconfigured domain names. Google Public DNS and Cisco OpenDNS were both patched to address this issue.

ELTIMA SDK

On December 7, Researchers from SentinelOne disclosed their research covering 27 vulnerabilities impacting the USB over ethernet driver found in Eltima software development kit (SDK) and derivative products using the library. The USB over ethernet driver allows users to redirect USB devices to their remote desktop. These vulnerabilities include both buffer and integer overflows and could be abused to achieve RCE with kernel-mode privileges. The Eltima SDK is used by a variety of cloud service providers including:

- Amazon Nimble Studio AMI
- Amazon NICE DCV
- Amazon WorkSpaces
- Amazon AppStream
- NoMachine
- Accops HyWorks
- Accops HyWorks DVM Tools
- Eltima USB Network Gate
- Amzetta zPortal Windows zClient
- Amzetta zPortal DVM Tools
- FlexiHub
- Donglify

The disclosure is careful to note that Eltima SDK may be used by other cloud providers that have not been evaluated. In some cases, these flaws affect both the client- and server-side applications, which means some customers will need to manually update their client applications. The vulnerability disclosure linked above contains recommendations and links to vendor responses for additional information on patching and mitigations. SentinelOne notes that no in-the-wild exploitation has been observed at the time their research was released. A list of the vulnerabilities and the products in which they were identified is included in the table below:

CVE	Product	Impact	CVSSv3
CVE-2021-42972	NoMachine Server	Buffer Overflow	8.8
CVE-2021-42973	NoMachine Server	Integer Overflow	8.8
CVE-2021-42976	NoMachine Enterprise Desktop	Buffer Overflow	8.8
CVE-2021-42977	NoMachine Enterprise Desktop	Integer Overflow	8.8
CVE-2021-42979	NoMachine Cloud Server	Integer Overflow	8.8
CVE-2021-42980	NoMachine Cloud Server	Buffer Overflow	8.8
CVE-2021-42983	NoMachine Enterprise Client	Buffer Overflow	8.8
CVE-2021-42986	NoMachine Enterprise Client	Integer Overflow	8.8
CVE-2021-42987	Eltima USB Network Gate	Integer Overflow	8.8
CVE-2021-42988	Eltima USB Network Gate	Buffer Overflow	8.8
CVE-2021-42990	FlexiHub For Windows	Buffer Overflow	8.8
CVE-2021-42993	FlexiHub For Windows	Integer Overflow	8.8

CVE	Product	Impact	CVSSv3
CVE-2021-42994	Donglify	Buffer Overflow	8.8
CVE-2021-42996	Donglify	Integer Overflow	8.8
CVE-2021-43000	Amzetta zPortal Windows zClient	Buffer Overflow	8.8
CVE-2021-43002	Amzetta zPortal DVM Tools	Buffer Overflow	8.8
CVE-2021-43003	Amzetta zPortal Windows zClient	Integer Overflow	8.8
CVE-2021-43006	AmZetta Amzetta zPortal DVM Tools	Integer Overflow	8.8
CVE-2021-43637	Amazon WorkSpaces agent	Buffer Overflow	8.8
CVE-2021-43638	Amazon Amazon WorkSpaces agent	Integer Overflow	8.8
CVE-2021-42681	Accops HyWorks DVM Tools	Buffer Overflow	8.8
CVE-2021-42682	Accops HyWorks DVM Tools	Integer Overflow	8.8
CVE-2021-42683	Accops HyWorks Windows Client	Buffer Overflow	8.8
CVE-2021-42685	Accops HyWorks DVM Tools	Integer Overflow	8.8
CVE-2021-42686	Accops HyWorks Windows Client	Integer Overflow	8.8
CVE-2021-42687	Accops HyWorks Windows Client	Buffer Overflow	8.8
CVE-2021-42688	Accops HyWorks Windows Client	Integer Overflow	8.8

DOMAIN NAME SERVER ECOSYSTEM

On May 11, researcher Mathy Vanhoef disclosed 12 vulnerabilities in Wi-Fi devices which he has named FragAttacks (fragmentation and aggregation attacks). These vulnerabilities impact all modern security protocols such as WPA3 and WEP. They do require user interaction or uncommon network configurations, making it harder for attackers to exploit.

CVE	Description	CVSSv3
CVE-2020-24586	Not clearing fragments from memory when (re)connecting to a network	3.5
CVE-2020-24587	Reassembling fragments encrypted under different keys	2.6
CVE-2020-24588	Accepting non-SPP A-MSDU frames	3.5
CVE-2020-26139	Forwarding EAPOL frames even though the sender is not yet authenticated	5.3
CVE-2020-26140	Accepting plaintext data frames in a protected network	6.5
CVE-2020-26141	Not verifying the TKIP MIC of fragmented frames	6.5
CVE-2020-26142	Processing fragmented frames as full frames	5.3
CVE-2020-26143	Accepting fragmented plaintext data frames in a protected network	6.5
CVE-2020-26144	Accepting plaintext A-MSDU frames that start with an RFC1042 header with EtherType EAPOL (in an encrypted network)	6.5
CVE-2020-26145	Accepting plaintext broadcast fragments as full frames (in an encrypted network)	6.5
CVE-2020-26146	Reassembling encrypted fragments with non-consecutive packet numbers	5.3
CVE-2020-26147	Reassembling mixed encrypted/plaintext fragments	5.4

INFRA:HALT

INFRA:HALT is a set of 14 vulnerabilities affecting the NicheStack Transmission Control Protocol/Internet Protocol (TCP/IP) stack. The impacts of these 14 vulnerabilities include RCE, DoS, information leakage, TCP spoofing and DNS cache poisoning. What's particularly interesting about NicheStack is that the earliest copyright messages suggest that the stack was first created in 1996. Because of its age, the stack has been used by multiple original equipment manufacturer's (OEMs) over a number of years, making it very difficult to determine the full scope of these flaws. There are potentially millions of devices affected by INFR:HALT due to the popularity of NicheStack, particularly in OT devices used in manufacturing. The following table outlines the 14 CVE's from this research.

CVE	Affected Component	Impact	CVSSv3
CVE-2020-25767	DNSv4	RCE	7.5
CVE-2020-25926	DNSv4	DNS cache poisoning	7.5
CVE-2020-25927	DNSv4	DoS	7.5
CVE-2020-25928	DNSv4	RCE	9.8
CVE-2020-35683	ICMP	DoS	7.5
CVE-2020-35684	TCP	DoS	7.5
CVE-2020-35685	TCP	TCP spoofing	9.1
CVE-2021-27565	HTTP	DoS	7.5
CVE-2021-31226	HTTP	RCE	9.8
CVE-2021-31227	HTTP	DoS	7.5
CVE-2021-31228	DNSv4	DNS cache poisoning	7.5
CVE-2021-31400	TCP	DoS	7.5
CVE-2021-31401	TCP	Application Dependent	7.5
CVE-2021-36762	TFTP	DoS	7.5

NAME:WRECK

NAME:WRECK is a set of nine vulnerabilities found across four TCP/IP stacks embedded in millions of devices. This research focused on domain name system (DNS) vulnerabilities with impacts ranging from DNS Cache Poisoning to DoS and RCE. DNS is a vital component of networking, providing a mapping between IP addresses and human readable domain names. The vulnerabilities identified in this research arise from implementation problems within the various TCP/IP stacks due to the complexities and misinterpretation of Request for Comments (RFC) standards. The following table contains a list of CVEs, the stack in which they were identified, the affected feature, their impact and CVSSv3 scores.

CVE	Stack	Affected Component	Potential Impact	CVSSv3
CVE-2016-20009	IPNet	Message compression	RCE	9.8
CVE-2020-15795	Nucleus NET	Domain name label parsing	RCE	8.1
CVE-2020-27009	Nucleus NET	Message compression	RCE	8.1
CVE-2020-27736	Nucleus NET	Domain name label parsing	DoS	6.5
CVE-2020-27737	Nucleus NET	Domain name label parsing	DoS	6.5
CVE-2020-27738	Nucleus NET	Message Compression	DoS	7.4
CVE-2020-7461	FreeBSD	Message Compression	RCE	7.3
CVE-2021-25677	Nucleus NET	Transaction ID	DNS Cache Poisoning	5.3
Not Assigned	NetX	Message Compression	DoS	6.5

NUCLEUS:13

NUCLEUS:13 is a set of 13 vulnerabilities found in Nucleus NET, the TCP/IP stack of the Siemens-owned Nucleus RTOS. Exploitation of these vulnerabilities can result in RCE, information disclosure and DoS. Four of the NUCLEUS:13 vulnerabilities were found in the file transfer protocol (FTP) or trivial FTP (TFTP) server used by the Nucleus RTOS. FTP is an insecure file transfer protocol, allowing plaintext authentication or in some cases no authentication, making it a prime target for attackers. CVE-2021-31886, the most critical vulnerability, can be easily exploited by sending a crafted username via the FTP USER command. When the username exceeds the allocated buffer size, a stack-based buffer overflow occurs resulting in a potential device crash (DoS) or allowing the attacker to control the execution flow and achieve RCE. The full list of CVEs is contained in the table below:

CVE	Affected Component	Potential Impact	CVSSv3
CVE-2021-31344	ICMP	Confused Deputy	5.3
CVE-2021-31345	UDP	DoS, Information leak. Impact depends on how UDP is implemented.	9.1
CVE-2021-31346	IP/ICMP	Information leak/DoS	9.1
CVE-2021-31881	DHCP Client	DoS	7.5
CVE-2021-31882	DHCP Client	DoS	7.5
CVE-2021-31883	DHCP Client	DoS	7.5
CVE-2021-31884	DHCP Client	DoS, Out-of-bound reads/writes. Impact depends on how the client is implemented.	9.8
CVE-2021-31885	TFTP Server	Information Leak	7.5
CVE-2021-31886	FTP Server	RCE	9.8
CVE-2021-31887	FTP Server	RCE	8.8
CVE-2021-31888	FTP Server	RCE	8.8
CVE-2021-31889	TCP Server	DoS	9.1
CVE-2021-31890	TCP Server	DoS	9.1

NUMBER:JACK

NUMBER:JACK is a set of nine vulnerabilities caused by the improper generation of initial sequence numbers (ISNs), which are used to ensure that a TCP connection between two devices is unique. Failure of an ISN to be unique could result in a collision, allowing a third party to interfere and hijack a connection by either spoofing or guessing the ISN. Exploitation of these flaws could result in DoS, authentication bypass or code injection. However, the actual impact can vary based on other protections that may be in place or on how an affected device is implemented. Of the 11 total stacks investigated, nine were found to be vulnerable as outlined in the table below.

CVE	Affected TCP/IP Stack	CVSSv3
CVE-2020-27213	Ethernut (Nut/Net)	7.5
CVE-2020-27630	uC/TCP-IP	7.5
CVE-2020-27631	CycloneTCP	7.5
CVE-2020-27632	NDKTCPIP	7.5
CVE-2020-27633	FNET	7.5
CVE-2020-27634	uIP/Contiki-OS/Contiki-NG	7.5
CVE-2020-27635	picoTCP	7.5
CVE-2020-27636	MPLAB Net	7.5
CVE-2020-28388	Nucleus NET	5.3

REALTEK

CVE-2021-35392 and CVE-2021-35393 are buffer overflow vulnerabilities originally discovered in Realtek chipsets for modems. CVE-2021-35394 is a command injection vulnerability and CVE-2021-35395 covers multiple flaws in the management web interface. The vulnerabilities exist in a Realtek Jungle SDK that is used in a variety of IoT devices. Researchers at IoT Inspector identified more than 65 vendors implementing the vulnerable SDK. Shortly after disclosure, these vulnerabilities were exploited to distribute a variant of the Mirai malware.

Qualcomm

QUALCOMM: CVE-2020-11261

CVE-2020-11261 is an improper input validation vulnerability in the Graphics component.

QUALCOMM: CVE-2021-1905

CVE-2021-1905 is a use-after-free vulnerability in the Graphics component.

QUALCOMM: CVE-2021-1906

CVE-2021-1906 is a detection of error condition without action vulnerability in the Graphics component.

CVE-2020-10148

CVE-2020-10148 is an authentication bypass flaw in the SolarWinds Orion API. According to CERT/CC, a remote attacker could exploit the vulnerability in order to execute API commands on the vulnerable Orion API instance. It is believed that this vulnerability was used to deploy the SUPERNOVA malware.

CVE-2021-35211

CVE-2021-35211 is a remote memory escape vulnerability in SolarWinds Serv-U Managed File Transfer Server. The flaw exists due to the way Serv-U has implemented the Secure Shell (SSH) protocol and can only be exploited if an organization has made the Serv-U SSH protocol externally accessible. If exploited, an attacker would be able to run arbitrary code with elevated privileges, which may include but is not limited to installing or executing malicious code, as well as accessing or altering data on the system.

CVE-2021-20021

CVE-2021-20021 is an improper privilege management vulnerability in SonicWall Email Security. An unauthenticated, remote attacker could exploit this vulnerability by sending a specially crafted HTTP request to a vulnerable host. Successful exploitation would allow the attacker to create an administrative account.

CVE-2021-20022

CVE-2021-20022 is an unrestricted upload of file with dangerous type vulnerability in SonicWall Email Security. An authenticated, remote attacker could exploit this vulnerability to upload malicious files to a vulnerable host.

CVE-2021-20023

CVE-2021-20023 is an arbitrary file read vulnerability in SonicWall Email Security. An authenticated, remote attacker could exploit this vulnerability to read arbitrary files from a vulnerable host.

CVE-2021-20016

CVE-2021-20016 is a critical SQL injection vulnerability in SonicWall's Secure Mobile Access 100 (SMA 100). A remote, unauthenticated attacker could submit a specially crafted query in order to exploit the vulnerability. Successful exploitation would grant an attacker the ability to access login credentials (username, password) as well as session information that could then be used to log into the vulnerable SMA appliance.

CVE-2021-20034

CVE-2021-20034 is an improper access control vulnerability in SMA 100. A remote, unauthenticated attacker could exploit this vulnerability by sending specially crafted requests to a vulnerable device to bypass path traversal checks. Successful exploitation would grant an attacker the ability to delete arbitrary files, which could result in a reboot to factory default settings.

SWISSLOG HEALTHCARE

PwnedPiper, is a set of nine vulnerabilities discovered in the Translogic pneumatic tube system (PTS). PTS systems are used in numerous hospitals to transport materials and documents via a series of pneumatic tubes. The impacts of the vulnerabilities include memory corruption bugs, privilege escalation, two hardcoded passwords, DoS and an unsigned firmware upgrade vulnerability. CVE-2021-37160, the most severe vulnerability from PwnedPiper, would allow an attacker to gain persistent access to a network by forcing the system to update using maliciously modified firmware that could be backdoored by an attacker. A list of the CVEs is found in the table below.

CVE	Description	CVSSv3
CVE-2021-37160	Unauthenticated, unencrypted, unsigned firmware upgrade	9.8
CVE-2021-37161	Memory corruption in the TLP20 protocol - Underflow in udpRXThread	9.8
CVE-2021-37162	Memory corruption in the TLP20 protocol - Overflow in sccProcessMsg	9.8
CVE-2021-37163	Two hardcoded passwords accessible through the Telnet server	9.8
CVE-2021-37164	Memory corruption in the TLP20 protocol - Off-by-three stack overflow in tcpTxThread	9.8
CVE-2021-37165	Memory corruption in the TLP20 protocol - Overflow in hmiProcessMsg	9.8
CVE-2021-37166	GUI socket Denial Of Service	7.5
CVE-2021-37167	Privilege escalation due to a user script being run by root	9.8

CVE-2021-21985

CVE-2021-21985 is a RCE in the vSphere Client via the Virtual SAN (vSAN) Health Check plugin, which is enabled by default. This vulnerability is assigned a CVSSv3 score of 9.8. To exploit this vulnerability, an attacker would need to be able to access vCenter Server over port 443. Even if an organization has not exposed vCenter Server externally, attackers can exploit this flaw once inside a network. VMware specifically calls out ransomware groups as being adept at leveraging flaws like this post compromise, after having gained access to a network via other means such as spearphishing. Successful exploitation would give an attacker the ability to execute arbitrary commands on the underlying vCenter host.

CVE-2021-21986

CVE-2021-21986 is an authentication mechanism issue in several vCenter Server Plug-ins, which is assigned a CVSSv3 score of 6.5. The affected vCenter Server Plug-ins include:

- vSAN Health Check
- Site Recovery
- vSphere Lifecycle Manager
- VMware Cloud Director Availability

CVE-2021-21986 can also be exploited via port 443 and allow an attacker to perform plugin functions without authentication.

CVE-2021-21972 AND CVE-2021-22005

CVE-2021-21972 and CVE-2021-22005 are both file upload vulnerabilities in vCenter Server. An unauthenticated attacker capable of accessing port 443 over the same network or directly from the internet could exploit a vulnerable vCenter Server by uploading a file to a vulnerable vCenter Server. Successful exploitation would result in remote code execution on the host. In its blog post, VMware notes that CVE-2021-22005 exists in vCenter Server "regardless of the configuration settings," which makes this exploitable by default on affected vCenter Server installations.

CVE-2021-21975

CVE-2021-21975 is a SSRF vulnerability in vRealize Operations, an AI-powered IT operations management platform for multi-cloud, private and hybrid environments. This vulnerability specifically affects the vRealize Operations API Manager and could allow a remote, unauthenticated attacker to steal administrative passwords.

CVE-2021-21983

CVE-2021-21983 is an arbitrary file write vulnerability in the vRealize Operations API Manager that could allow an authenticated remote attacker to write files (potentially malicious in nature) to arbitrary locations on VMware's underlying OS. While exploiting this vulnerability on its own would require authentication, the attacker can bypass this requirement by chaining CVE-2021-21975

ZOHO

CVE-2021-40539

CVE-2021-40539 is a REST API authentication bypass vulnerability in ManageEngine ADSelfService Plus. A remote, unauthenticated attacker could exploit this vulnerability by sending a specially crafted request to a vulnerable host. Successful exploitation would grant an attacker remote code execution. In November 2021, CISA and the FBI issued an alert about an APT group exploiting this flaw.

CVE-2021-44515

CVE-2021-44515 is an authentication bypass vulnerability in ManageEngine Desktop Central that could lead to remote code execution. To exploit, an attacker would send a specially crafted request to a vulnerable endpoint.

About the Tenable Security Response Team

Tenable Research seeks to step out in front of the curve of the vulnerability management cycle. Our Security Response Team tracks threat and vulnerability intelligence feeds to make sure our plugin teams can deliver coverage to our products as quickly as possible. The SRT also works to dig into technical details and author white papers, blogs, and additional communications to ensure customers are fully informed of the risks. The SRT provides breakdowns for the latest vulnerabilities on the Tenable blog.

Tenable Research has released over **166,000 plugins** and leads the industry on CVE coverage. The team is focused on diverse work that makes up the foundations of vulnerability management: writing plugins for vulnerability and asset detection; developing audit and compliance checks; improving VM automation.

About the Authors

Scott Caveza, Research Engineering Manager

Satnam Narang, Staff Research Engineer

Claire TIlls, Senior Research Engineer

Additional Credits:

Susan Nunziata, Senior Director of Editorial & Content

Brooke Fox, Marketing Manager

Felix Do, Graphic Designer

Maya Smith, Senior Creative Director

6100 Merriweather Drive
12th Floor
Columbia, MD 21044

North America +1 (410) 872-0555

www.tenable.com

01/13/22 V05

COPYRIGHT 2022 TENABLE, INC. ALL RIGHTS RESERVED. TENABLE, TENABLE.IO, NESSUS, ALSID, INDEGY, LUMIN, ASSURE, AND LOG CORRELATION ENGINE ARE REGISTERED TRADEMARKS OF TENABLE, INC. OR ITS AFFILIATES. TENABLE.SC, TENABLE.OT, TENABLE.AD, EXPOSURE.AI, AND THE CYBER EXPOSURE COMPANY ARE TRADEMARKS OF TENABLE, INC. OR ITS AFFILIATES. ALL OTHER PRODUCTS OR SERVICES ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS.